биологическая ценность и аминокислотный состав готового продукта. В результате было установлено, что показатели биологической ценности белкового компонента приготовленных колбас имеют более высокое значение, чем контрольные. При исследовании качественных показателей и биологической ценности колбасных изделий продукция опытного образца была на 5,21% выше контрольного образца по массовой доле белков.

***Ключевые слова**: тыква-белково-углеводный комплекс, вареная колбаса, рецептура, аминокислотный состав, белковый компонент, биологическая ценность.*

STUDY OF INDICATORS OF QUALITY AND BIOLOGICAL VALUE OF THE DEVELOPED MEAT AND CEREAL SAUSAGE

S. Zhumabekov, Sh. Abzhanova, A. Katasheva, B. Jetpisbayeva

In the article, one of the criteria for evaluating their formulas in the development of new types of meat products is the formulation of sausage products with pumpkin protein and carbohydrate complex to normalize the chemical composition of the product in terms of the optimal ratio of protein and fat. To confirm the importance of using the pumpkin-protein-carbohydrate complex, as well as the correctness of the selected level of their introduction, the nutritional and biological value and amino acid composition of the finished product were studied. As a result, it was found that the indicators of the biological value of the protein component of cooked sausages have a higher value than the control ones. When studying the quality indicators and biological value of sausage products, the production of the prototype was 5.21% higher than the control sample in terms of the mass fraction of proteins.

***Key words:** pumpkin-protein-carbohydrate complex, boiled sausage, recipe, amino acid composition, protein component, biological value.*

МРНТИ: 81.93.29

Б.С. Ахметов[1], В.А. Лахно[2], А.К. Шайханова[3], Ш.Д. Толыбаев [4,5]
[1]Казахский национальный педагогический университет имени Абая, г. Алматы
[2]Национальный университет биоресурсов и экологических наук Украины, г. Киев
[3]Семей қаласының Шәкәрім атындағы университеті
[4]Алматы энергетика және байланыс университеті
[5]Казахский национальный университет имени аль-Фараби, г. Алматы

КИБЕРҚАУІПСІЗДІК МӘСЕЛЕЛЕРІНДЕГІ КИБЕРҚАУІП БЕЛГІСІНІҢ МАТРИЦАСЫ НЕГІЗІНДЕ ШЕШІМДЕРДІ ҚОЛДАУ

***Аңдатпа:** Ақпараттық технологиялар мен жүйелерді қолдану масштабтарының жаһандануына байланысты, олардың үздіксіз жұмыс жасауын қамтамасыз етудегі ең басты мәселе – деструктивті және рұқсат етілмеген басып кірулерден электронды ресурстардың киберқауіпсіздігі мен ақпараттық қауіпсіздігі. Мақалада киберқауіптер мен ауытқуларды (аномалии) танып білу мәселелеріндегі интеллектуалдандырылған шешімдерді қолдау жүйесінің (ИШҚЖ) білім базасында сапалық кеңістікті құру алгоритмі мен әдісі баяндалды. Әзірленіп жатқан ИШҚЖ-сін автономды түрде киберқауіпсіздік қызметтерінің аналитиктері, сонымен қатар ақпаратты қорғау жүйелерінде кешенді түрде де қолдануға болады. Ұсынылған алгоритмдер жаңа қауіптер пайда болған сайын білім қорын динамикалық түрде толтыра отырып, қауіптерді, әсіресе, сапалары қиын түсіндірілетін қауіптерді анықтау мен анализдеу уақытын қысқартуға және ақпараттандыру объектілеріне төнетін шабуылдарды, ауытқуларды (аномалии), қауіптерді табу жүйелерінің жалған іске қосылу санын азайтуға мүмкіндік береді.*

***Түйін сөздер**: киберқауіпсіздік, қауіптер, шешімдерді қолдау, білім қорын құру алгоритмі.*

Кіріспе

Ақпараттық технологиялар мен жүйелерді қолдану масштабтарының жаһандануына байланысты, олардың үздіксіз жұмыс жасауын қамтамасыз етудегі ең басты мәселе – деструктивті және рұқсат етілмеген басып кірулерден электронды ресурстардың киберқауіпсіздігі (КрҚ) мен ақпараттық қауіпсіздігі (АҚ).

Айтарлықтай, ертеден-ақ, әр түрлі желілік басып кірулерді анықтау немесе танып білу, сонымен қатар шабуылдар мен ауытқулардың (аномалия) сапасын анықтау жүйелері КрҚ нарығында өз тауашасына (ниша) ие [1–3].

АҚ пен ҚрҚ-тің қауіптерін анықтаудың интеллектуалдандырылған жүйесін әзірлеу, әсіресе, аса маңызды компьютерлік желілер (МКЖ) үшін әзірлеу жаңа бағытқа айналды [3, 4]. Сонымен қатар, мұндай программалық өнімдердің айтарлықтай бөлігі шешімдерді қолдау жүйелер (ШҚЖ) [4] немесе сараптаушы жүйелердің (СЖ) [5-7] модульдерінен тұрады. Бұл модульдер кәсіпорындардың, ұйымдардың тағы да басқа аса маңызды компьютерлік желілердің ақпараттық-коммуникациялық жүйелеріне күрделі шабуыл жасалған кездері КрҚ және ақпаратты қорғау (АҚ) қызметтеріндегі аналитиктердің шешім қабылдау мен анализдеу жылдамдығын тиімді жоғарылатуға мүмкіндік береді [7-9].

Көптеген зерттеушілер тәжірибеде өзін көрсете білген классикалық әдістерді әлеуетті біріктіруге қабілетті аралас әдіспен, сонымен қатар жаңа немесе жетілдірілген киберқауіптерді тиімді және адекватты анықтауға қабілетті жаңа әдістермен байланысты болған бағыттың болашағы бар деп есептейді [2]. Сонымен бірге, интеллектуалдандырылған СЖ мен ШҚЖ сияқтылардың танып білу рәсімдерінде жеткілікті дәрежеде қатыспауымен байланысты болған және (кибершабуыл, ауытқу мен киберқауіптерді) танып білу объекттері сипатының күрделіленуімен байланысты болған қарама-қайшылықтарды шешуге болады. Демек, ақпараттық-коммуникациялық жүйелердегі (АКЖ) (немесе ақпараттандырудың өзге де объектілерінде АОБ) ауытқулар мен қауіптерді бағалау үшін, әсіресе, киберқауіптер, ауытқулар, мен шабуылдар туралы берілетін жаңа мәліметтер төмен ұйымдастырылған кездері ИШҚЖ-леріне арналған жаңа модельдерді әзірлеу релеванттық мәселе болып қалады.

1. Алдыңғы зерттеулердің анализі және әдебиеттерге шолу

Жоғарыда көрсетіп өткеніміздей, әр түрлі АОБ-де ИКЖ-ге киберқаскүнемдердің деструктивті әсер етуінің саны мен күрделілігінің жоғарылауы әлемдік тендециямен анықталғандығының өзі зерттеуіміздің өзектілігін көрсетеді. Осы АОБ-лердегі кибершабуылдарды өткізу сценарийлерінің күрделіленуі мен санының өсуі, сонымен қатар киберқауіптердің нұсқалылығы киберқауіптерді, ауытқуларды және кибершабуылдарды интеллектуалды тиімді танып білу жүйелерін (КАКИТЖ) әзірлеуге деген қызығушылық туғызды [1, 2, 11, 12]. АҚ пен КрҚ саласындағы СЖ [5, 7, 13–16] мен ИШҚЖ-ге [2, 4, 12] арналған модельдерді, әдістерді және программалық қамтаманы (ПҚ) дамыту бойынша жүргізілетін жұмыстар, бұл саладағы зерттеулердің бір бағыты болып табылады.

Авторлардың пікірінше [18, 19], АОБ-ның қорғану дәрежесін анализдеу мен таргетивті кибершабуылдарға қарсы құрылытын жоспардан бұрын негізгі қауіптер мен әлсіздіктерді анықтау кезеңі болуы қажет. Осы пікірлеріне қарамастан, зерттеушілер АОБ ИКЖ-леріндегі қауіптер мен әлсіздіктер арасындағы байланысты рәсімдеу мәселесі қиын екендігін көрсетіп өтеді.

Жұмыстарында АҚ пен КрҚ саласындағы СЖ мен ИШҚЖ-дің кемшіліктері қарастырылады. Мұндай кемшіліктерге: білім базасын (ББ) және білім аясын (БА) құру барысында біліктілігі жоғары сарапшы болуы қажет; бір бөлек әдістер мен модельдерді алгоритмдеу қиындығы; нақты ИШҚЖ-нің тиімділігін бағалау мүмкіндігі жоқтығы т.б. жатады [19, 20].

Осылай, қаралған жұмыстардағы пікірталастарды қарастыра отырып, зерттеуімізді жүзеге асырылатын АОБ КрҚ саласындағы ИШҚЖ-не арналған алгоритмдер мен модельдер бойынша жалғастыру қажет екені айқындалды.

2. **Зерттеу жұмысының мақсаты мен міндеттері**

Мақсаты – әр түрлі ақпараттандыру объектілерінің электрондық ресурстары үшін киберқауіптерді танып білу мен анықтау барысында интеллектуалдандырылған шешімдерді қолдау жүйесі үшін модельдер мен әдістерді әзірлеу.

Зерттеу мақсатына жету үшін келесі міндеттер қойылады:

- АОБ КрҚ-ті алғашқы сипаттау үшін кеңістік сапасын жылдам жасауға мүмкіндік беретін ИШҚЖ үшін алгоритмдер мен әдістер әзірлеу;
- нақты АОБ үшін жаңа киберқауіптер жіктелуімен байланысты болған мәселелерді шешу және киберқауіптерді жылдам жіктеу үшін алгоритмдерді әзірлеу.

3. Модельдер мен әдістер

ИШҚЖ қауіптер туралы білім базасы (ББ) «Объект – сапа» кестесіне негізделген. Жолдар (строка) танып білу объектілерін (ТО) сипаттайды, мысалы, қауіпті, ауытқуды немесе кибершабуыл тобын. Жолдар – ТО сапалары (немесе AT белгілері). Шамамен, егер

$k-$ ТО-сі танып білуге және жіктеуге қажетті сапасы/белгісі бар болса, онда сәйкесінше жол элементі – $j-$ бірге («1») тең. Егер $j-$ нольге («0») тең болса, онда ББ-гі ТО-сінің сапасы жоқ немесе ТО-ін жіктеу рәсімін жүргізу үшін параметрлері жеткіліксіз. ББ-де кесте жолдары былай берілген:

$$RO_i[at(i), at(j), at(k)], \quad (1)$$

мұндағы $at = \{1,0\}$ – белгі мәні (сапа); $i, j, k-$ ТО-не арналған белгілер (объекттегі тәртіп ретімен келетін сапалар саны, мысалы і номерлі киберқауіп – RO_i) саны.

МКЖ мен АОБ үшін киберқауіптердің қауіптерінің жіктелу алгоритмдері мен модельдері ИШҚЖ-нің негізгі себеп болды.

Сапа кеңістіктері мен ИШҚЖ білім базасын құру алгоритмдері үшін алғышарттар мен алғашқы мәліметер:

қабылданды: $TO = \{TO_1 : (i = 1,2,...m)\}$ – АОБ КрҚ (немесе МКЖ) қауіптердің эталонды объекттер жиынтығы $\{TH1, TH2, ...THk\}$, мұндағы $TH_i = (RO_i^1, RO_i^2, ..., RO_i^n)$; $RO_i^1 - j$ - АОБ КрҚ (немесе МКЖ) қауіпінің $i-$лі объект сапасы;

2) ТО $n-$ өлшемді вектор $TH_i = (X_i^1, X_i^2, ..., X_i^n)$ түрінде анықталады; мұндағы $\{X_i^1, X_i^2, ..., X_i^n\}-$ АОБ КрҚ (немесе МКЖ) қауіпінің сапа кеңістігіндегі мүмкін болған сапалар жиыны;

AL1 алгоритмі үшін эталонды объект жиынтығын $\{TH1, TH2, ...THk\}$ және дәрежелері бірдей жолдар үшін екілік формата берілген ТО береміз. Әрбір «1» екілік дәрежесі белгілі бір сапаға сәйкес келеді. «0» екілік дәрежесі – жоқ екеніне сәйкес келеді;

$TH_u, (u = 1,2,..., k)$ эталонды объектісінің $\psi(TH_u, TH)$ сәйкес келу функциясын және сәйкесінше сапаларға (TH) ТО береміз:

$$\psi(TH_u, TH) = \begin{cases} 1 \; if \; l - (TH_u, TH) \le h < l; \\ 0 \; if \; h < l - (TH_u, TH), \end{cases} \quad (2)$$

мұндағы $l-$дәрежелі жолдар ұзындығы; $h = l - 2$ – екілік дәрежелер саны; $(TH_u, TH)-$ TH_u, TH векторларының скаляр көбейтіндісі;

ИШҚЖ ББ-дағы жаңа объекттерді, сонымен қатар қолда бар объекттерді жіктеу; алғашқы (МКЖ мен АОБ КрҚ қауіптері) ТО жиынтығын қиылыспайтын жиынтықтарға (яғни, топтарға) бөлу рәсімі арқылы жіктеуге болады;

Жоғарыда келтірілген рәсім алгоритмдік шешу ережесіне, сонымен қатар [3, 18, 21, 22] жұмыстарында біздің берген модельдерге сүйене отырып жасалынған болатын;

ИШҚЖ арналған шешуші ереже келесі жағдайларға бола құрылған: егер номері 1 объект жолында сәйкес келетін екілік дәрежелер көп болса немесе номері 2 объект жолындағы екілік дәрежелілер берілген санға тең келсе, екі объект жақын деп есептеледі; ТО сипатында $n-$ өлшемді кеңістік пен «ұқсас емес» арасында өзара бірмәнді сәйкестік бар; ББ символдары мен ТО сапасының мәндері «1» мен «0» тең.

Киберқауіптерді танып білу бойынша объектіні жіктеу мына тізбекте орындалды (бұрын ИШҚЖ ББ-де сипатталмаған):

Белгісіз ТО-ні анализдеу үшін сигнатура белгілеп қоямыз, яғни жіктеу объектісі – OCL.

Жіктеліп жатқан ТО сигнатурасын RS1 (яғни, RS – бұл тірек сигнатура) салыстырамыз. Егер OCL RS1 жақын болса, онда осы тірек сигнатураға сәйкес келуші дәреже, «1» мәнін алады. Ал керсінше болса, онда – «0».

3. ОР сигнатурасын RS2 мен салыстыру жүзеге асырылады. Егер OCL RS2 жақын болса, онда осы RS сәйкес келетін дәреже, «1» мәніне ие болады. Ал керсінше болса, онда – «0».

4. Бұр рәсім анализдеуден өтіп жатқан объекттердің барлығының RS пен салыстырылуы аяқталғанға дейін жалғасады.

5. Осылай алынған кейбір объектілердің екілік жолдары осы OCL үшін келесіде сигнатура болып келеді. ИШҚЖ ББ-дағы бірдей сигнатуралары бар объекттердің барлығы бір топқа жатады. Осылай, сигнатура осы топтың «атауына» айналады.

Алгоритм әрбір объектіге бір сигнатура тіркейді, сонымен қатар сигнатура санын анықтауға мүмкіндік береді. Бұл сигнатуралары бірдей барлық объектілерді топтастыруға мүмкіндік береді. ТО танып білудің тиімді нәтижесіне кепіл беретін, жеткілікті эталонды нұсқалар санын эксперимент арқылы іріктеп алуға болады, мысалы, h (яғни ұқсастық шегі) параметрін өзгерту арқылы алуға болады. Немесе алдыңғы [3, 18, 21–25] жұмыстар арқылы, есептеп шығару көлемін қысқарту мақсатымен әдістер мен модельдерді қолдану, олар сапасы бар матрицаның көлемін кішірейтуге көмек береді [21].

4. Эксперимент

MATLAB-да жүргізілген тәжірибелік зерттеулер негізінде екі кезңде жұмыс жасайтын *AL1*, *AL2* біріктіру қажеттігі туралы нәтиже алынды. Бірінші кезеңде еркін ТО-ні танып білу үшін *AL2*, сосын *AL1* алгоритмі қолданылды. Нәтижелерді түзеткеннен кейін ТО-ні топтарға жатқызу туралы соңғы нәтижелер қалыптасты. Бұл ИШҚЖ-дегі *AL1*, *AL2* алгоритмдердің жұмыс жасауы кезіндегі қателер санын минимумдастыруға, орнын толтыруға мүмкіндік береді.

Осы зерттеу нәтижелерін енгізгеннен кейінгі мүмкіндіктер: бар болған, жасалып жатқан, жаңартылып жатқан киберқорғаудың кешенді жүйелерінің функционалдық мүмкіндіктері кеңейтуге болады; АОБ-де деструктивті әсер ету санының өсуі кезінде шешімдерді қабылдаудың жылдамдығы мен сапасын көтеруге болады; ИШҚЖ on-line режимде жұмыс жасауының есебінен аймақтық қашықтықтағы сарапшылар мен аналитиктердің мүмкіндігін АҚ арқылы іске қосуға болады [21-23].

Қорытынды.

Мақалада зерттеуіміздің келесі негізгі, нақтырақ айтсақ, бірінші рет әзірленіп, жетілдірілген нәтижелері сипатталады:

- ақпараттық ресурстардың киберқауіптерін танып білудің сапалық кеңістігін құрудың алгоритмдері мен әдісі; киберқауіптің бейімделген сапалық кеңістігіне және қауіптердің эталонды топтар жүйесіне негізденетін (қолданылып жүргеннен ерекшелігі)
- әр түрлі топтағы қауіптердің жүзеге асырылуынан кейінгі, әсіресе, әлсіз құрастырылған киберқауіп сапасы туралы мәліметтер болған кездегі жағдайды және аса маңызды компьютерлік жүйелердегі ауытқуларды бағалау үшін интеллектуалдандырылған бейімделген шешімдерді қабылдауды қолдау жүйесі құрамында киберқауіптерді анализдеу алгоритмі.

Бұл алгоритм, өзге алгоритмдерден ерекше, себебі белгілі топтар шеңберінде қауіптерді танып білу міндетін бір бөлек қарастыруға мүмкіндік береді де, қажет болған кездері сапалық кеңістікті жаңадан туындаған қауіптің типтеріне қарай толықтыруға мүмкіндік береді.

Жұмыс «Ақпараттандырудың аса маңызды объектілерінің киберқауіпсіздік саласындағы бейімделген сарапшылық жүйелерін әзірлеу» (ИРН: AP05132723) жобасының гранттық қаржыландыруы негізінде орындалды.

Әдебиеттер

1. Petit J., Shladover S.E. Potential Cyberattacks on Automated Vehicles, IEEE Transactions on Intelligent Transportation Systems. − 2015. − Vol. 16, Iss. 2. − P. 546-556.
2. Miao F., Zhu Q., Pajic M. G., Pappas J. Coding Schemes for Securing Cyber-Physical Systems Against Stealthy Data Injection Attacks, IEEE Transactions on Control of Network Systems. – 2016. − Vol. PP, Iss. 99. − P. 1.
3. Petrov B., Borowik M., Karpinskyy Immune and defensive corporate systems with intellectual identification of threats // Pszczyna: Śląska Oficyna Drukarska. – 2016. − P. 222
4. Sawik T. Selection of optimal countermeasure portfolio in it security planning, Decision Support Systems. – 2013. − Vol. 55, Iss. 1. − P. 156–164.
5. Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F. Decision support approaches for cyber security investment // Decision Support Systems. – 2016. − Vol. 86. − P. 13-23.
6. Atymtayeva L., Kozhakhmet K., Bortsova G. Building a Knowledge Base for Expert System in Information Security // Chapter Soft Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing. – 2014. − Vol. 270. − P. 57-76.

7. Gamal M.M., Hasan B., Hegazy A.F. A Security Analysis Framework Powered by an Expert System // International Journal of Computer Science and Security (IJCSS), 2011, − Vol. 4, − No. 6, P. 505-527.
8. Dua S., Du X. Data Mining and Machine Learning in Cybersecurity // UK, CRC press. – 2016. − P. 225.
9. Buczak A.L., Guven, E.A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. – 2016. − Vol. 18, − Iss. 2. – P. 1153-1176.
10. Al-Jarrah, O., Arafat, A. Network Intrusion Detection System using attack behavior classification // 5th International Conference on Information and Communication Systems (ICICS). − 2014.
11. Ben–Asher, Gonzalez, N. C. Effects of cyber security knowledge on attack detection // Computers in Human Behavior. – 2015. − Vol. 48. − P. 51-61.
12. Nishanov A. Kh, Kerimov K.F. Methods of Counteraction from Attacks Carried out Against Users in a Network the Internet // ICEIC-Electronics, news and communications, IX-the conference. − Tashkent, 2008. − P. 298-299.
13. Gamal M.M., Hasan B., Hegazy A.F. A Security Analysis Framework Powered by an Expert System // International Journal of Computer Science and Security (IJCSS). – 2011. − Vol. 4, No. 6. − P. 505-527.
14. Chang Li-Yun, Lee Zne-Jung Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system // International Conference on Fuzzy Theory and Its Applications. – 2013. − P. 346-351.
15. Kanatov M. Atymtayeva L., Yagaliyeva B. Expert systems for information security management and audit, Implementation phase issues, Soft Computing and Intelligent Systems (SCIS) // Joint 7th International Conference on and Advanced Intelligent Systems (ISIS). – 2014. − P. 896-900.
16. Lee Kuo-Chan, Hsieh C.-H., Wei L.-J., Mao C.-H., Dai J.-H., Kuang Y.-T Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation // Soft Computing. – 2016. − P. 1-14.
17. Pan S., Morris T., Adhikari U. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems // IEEE Transactions on Smart Grid. – 2015. − Vol. 6, Iss. 6. − P. 3104-3113.
18. Lakhno V., Kazmirchuk S., Kovalenko Y., Myrutenko L., Zhmurko T. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features // Eastern-European Journal of Enterprise Technologies. – 2016. − No 3/9(81). − P. 30-38.
19. Louvieris P., Clewley N., Liu X. Effects-based feature identification for network intrusion detection // Neurocomputing. – 2013. − Vol. 121, Iss. 9. − P. 265-273.
20. Wang Z., Zhou X., Yu Z., He Y., Zhang D. Inferring User Search Intention Based on Situation Analysis of the Physical World // Chapter Ubiquitous Intelligence and Computing. – 2010. − Vol. 6406. − P. 35-51.
21. Lakhno V. Zaitsev S., Tkach Y., Petrenko T. Adaptive Expert Systems Development for Cyber Attacks Recognition in Information Educational Systems on the Basis of Signs' Clustering // Part of the Advances in Intelligent Systems and Computing book series (AISC). – 2018. − Vol. 754. − P. 673-682.
22. Akhmetov B., Lakhno V., Boiko Y., Mishchenko A. Designing a decision support system for the weakly formalized problems in the provision of cybersecurity // Eastern-European Journal of Enterprise Technologies. – 2017. − Vol. 1, Issue 2 (85). − P. 4-15.
23. Lakhno V., Akhmetov B., Korchenko A., Alimseitova Z., Grebenuk V. Development of a decision support system Based on expert evaluation for the situation center of transport cybersecurity // Journal of theoretical and applied information technology. – 2018. − Vol.96. No 14. − P. 4530-4540.
24. Al Hadidi M., Ibrahim Y. K., Lakhno V., Korchenko A., Tereshchuk A., Pereverzev A. // Intelligent systems for monitoring and recognition of cyber attacks on information and communication systems of transport. International Review on Computers and Software. – 2016. − Vol. 11, No 12. − P. 1167-1177.
25. Beketova G., Akhmetov B., Korchenko A., Lakhno A. Simulation modeling of cyber security systems in MATLAB and SIMULINK // Bulletin of the national academy of sciences of the republic

of Kazakhstan. – 2017. − Vol. 3. − P. 54-64.

ПОДДЕРЖКА РЕШЕНИЙ В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ НА ОСНОВЕ МАТРИЦ ПРИЗНАКОВ КИБЕРУГРОЗ

Б.С. Ахметов, В.А. Лахно, А.К. Шайханова, Ш.Д. Толыбаев

В связи с глобализацией масштабов применения информационных технологий и систем, главной проблемой обеспечения их бесперебойного функционирования является кибербезопасность электронных ресурсов и информационная безопасность от деструктивных и несанкционированных вторжений.Системы обнаружения или распознавания различных сетевых вторжений, а также определения качества атак и аномалий имеют свою нишу на рынке. В данной работе описан метод и алгоритмы формирования признакового пространства для базы знаний интеллектуализированной системы поддержки решений в задачах кибербезопасности. Интеллектуализированная система поддержки решений может использоваться совместно с комплексными системами защиты информации. Описанные алгоритмы, позволяют динамически пополнять базу знаний при появлении новых угроз, что позволит сократить время их выявления и анализа, в тот же момент для случаев труднообъяснимых признаков и уменьшить количество ложных срабатываний в системах обнаружения угроз, аномалий и атак на объекты информатизации.

***Ключевые слова**: кибербезопасность, угрозы, поддержка решений, алгоритм формирования базы знаний.*

DECISION SUPPORT IN CYBERSECURITY PROBLEMS BASED ON MATRIX OF SIGNS OF CYBERTHREATS

B. Akhmetov, V. Lakhno, A. Shaikhanova, SH. Tolybayev

Due to the globalization of the use of information technologies and systems, the main problem of ensuring their smooth functioning is the cybersecurity of electronic resources and information security from destructive and unauthorized intrusions. Systems for detecting or recognizing various network intrusions, as well as determining the quality of attacks and anomalies, have their own niche in the market.This paper describes a method and algorithms for the formation of a feature space for the base of an intellectualized decision support system in cybersecurity problems. Intellectualized support system for promoting the protection of information about yourself with complex systems. The described algorithms allow you to dynamically replenish the database when new threats appear, which will reduce the time for their analysis, at the same time for cases of difficult-to-explain symptoms and reduce the number of false positives in the system for detecting threats, anomalies and attacks on information objects.

***Key words:** cybersecurity, threats, decision support, knowledge base generation algorithm.*