УДК 004.056
https://doi.org/10.47533/2020.1606-146X.136

Б. С. АХМЕТОВ[1], В. А. ЛАХНО[2], М. Б. ЫДЫРЫШБАЕВА[3]*, А. К. АБУОВА[4], Ш. САГЫНДЫКОВА[5]

[1]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Қазақстан
[2]Украинаның Ұлттық биоресурстар және табиғатты пайдалану университеті, Киев, Украина
[3]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
[4]Қазақ теміржол көлігі университеті, Алматы, Қазақстан
[5]Алматы энергетика және байланыс университеті, Алматы, Қазақстан

КИБЕРШАБУЫЛДАРДЫҢ САЛДАРЫН БАҒАЛАУҒА АРНАЛҒАН ШЕШІМ ҚАБЫЛДАУДЫ ҚОЛДАУ ЖҮЙЕСІ

Байес желілерін (БЖ) қолдану арқылы есептерді шешу үшін аномалиялар мен кибершабуылдар белгілері туралы деректерді талдауға әзірленген Bayesian_Net шешім қабылдауды қолдау жүйесінің (ШҚҚЖ) архитектурасы сипатталған. Ұсынылған ШҚҚЖ объектіге бағытталған бағдарламалауды қолданумен ерекшеленеді және модульдік архитектураға ие. Bayesian_Net ШҚҚЖ деректерді интеллектуалды талдау есептерін шешуге, атап айтқанда ақпараттандыру объектілерінің (АО) кибернетикалық қауіпсіздігімен (КҚ) байланысты әлсіз құрылымдалған мәселелерді талдауға және белгілер мен анықталған ауытқулар туралы әлсіз құрылымдалған деректер жағдайында кибершабуылдардың салдарын бағалауға арналған.

Түйін сөздер*: Байес желісі, кибернетикалық қауіпсіздік, шешім қабылдауды қолдау жүйесі, бағдарламалық өнім.*

Кіріспе. Ақпараттандыру объектілеріне (АО) бағытталған шабуылдарды жүргізу сценарийлерінің күрделілігінің өсуіне қарай кибернетикалық қауіпсіздік (КҚ) саласында шешімдер қабылдау барынша күрделі міндетке айналуда. Сонымен қатар, оны шешу үшін КҚ саласының сарапшылары арнайы әдебиеттерде аз сипатталған немесе алғаш рет кездесетін жаңа қауіптерді талдау үшін әлсіз құрылымдалған деректермен (ӘҚД) жұмыс жасауына тура келеді. Мақсатты (таргеттелген) шабуылдарды жүргізу барысында хакерлер көбінесе бірегей зиянды бағдарламалар мен АО-ға ену әдістерін жиі қолданады. АО-ға заңсыз әсер ету күрделілігінің тұрақты өсуіне, ақпаратты қорғау жүйелерінің құрылымына біріктірілген шешімдерді қолдау жүйелерінің (ШҚҚЖ) модульдері бар аномалиялар мен кибернетикалық шабуылдарды интеллектуалды тану жүйелерін қолдана отырып қарсы тұруға болады.

Алдыңғы зерттеулерге шолу. АО-де кибершабуылдар санының өсуі соңғы жылдары АҚ және КҚ саласындағы КҚ [1, 2] міндеттері бойынша тиімді ШҚҚЖ әзірлеуге қызығушылық тудырды.

[3, 4] жұмыстарда АҚ және КҚ есептерінде Data Mining технологиялары қарастырылды. Бұл зерттеулерде АО КҚ қамтамасыз етумен байланысты жағдайлардың эволюциясының заңдылықтарын анықтауға баса назар аударылады. Қарастырылған жұмыстарда бағдарламалық кешендер тәжірибе жүзінде іске асырылмады.

* E-mail корреспондирующего автора: moldir.ydyryshbaeva@gmail.com

[5, 6] жұмыстарда АО КҚ есептерінде интеллектуалды модельдеу әдістемесі талданады. Авторлар ұсынған әдістеме ақпаратты қорғаудың (АҚ) жеткіліксіз құрылымдалған жағдайларын талдауға және шешім қабылдауға арналған. Алайда, бұл зерттеулер аппараттық немесе бағдарламалық құрал ретінде жүзеге асырылмаған.

[7-11] жұмыстарда белгілер мен анықталған аномалиялар туралы ӘҚД жағдайында кибершабуылдардың салдарын бағалау үшін БЖ қолданудың орындылығы туралы қорытынды жасалды.

Мақаланың негізгі материалы. Зерттеу барысында әзірленген ШҚҚЖ себеп-салдарлық байланыстарды талдау, жіктеу, кластерлеу, болжау және визуализация сияқты киберқауіпсіздікке (КҚ) байланысты міндеттерді шешуге бағытталған компьютерлік жүйе болып табылады. Бұл міндеттерді шешу бұрын сарапшылардан алынған оқу деректері бойынша сарапшылардың қатысуынсыз жүзеге асырылады. Сарапшылардың қатысуы шабуыл белгілері ӘҚД жағдайында талдау жүргізу ғана қажет. Әзірленген ШҚҚЖ-ның негізгі міндеті – шешім қабылдаушы тұлғаға көмек көрсету (ШҚТ). Әзірленген ШҚҚЖ «Bayesian_Net» атауын алды. Bayesian_Net техникалық тұрғыда десктопты бағдарламалық жасақтама (бағдарламалық қамтамасыз ету) санатына жатады, өйткені ол пайдаланушының тек бір компьютеріне қызмет етеді және әдепкі қалпы бойынша желіге қосылмаған. Bayesian_Net – бұл белсенді ШҚҚЖ, яғни ол пайдаланушыға қорғалатын желіде белгілі бір оқиғаның пайда болу ықтималдығының алынған мәндері негізінде шешім қабылдауына көмектеседі.

Bayesian_Net жартылай автоматты режимде БЖ түріндегі модельдерді құруға және шабуылдардың белгілері бойынша қолда бар деректер негізінде сәйкес ықтималдық қорытындыны қалыптастыру арқылы жіктеу, кластерлеу және болжау мәселелерін шешуге қабілетті.

Дайындалған Bayesian_Net ШҚҚЖ блок-схемасы 1-суретте көрсетілген. Bayesian_Net ШҚҚЖ үш негізгі ішкі жүйеден тұрады және блоктық-модульдік архитектураға ие.

Енгізу-шығару құрылғылары пайдаланушыға БЖ құру және жасырын төбелердің параметрлерін үйрету үшін деректерді жүктеуге, сонымен қатар жұмыс нәтижелерін сыртқы файлдарға сақтауға мүмкіндік береді.

Интерфейстің ішкі жүйесі пайдаланушыны, Bayesian_Net ШҚҚЖ ішкі элементтерімен, сыртқы сақтау құрылғыларымен және енгізу-шығару құрылғыларымен байланыстырады. Интерфейс пайдаланушыға деректерді жүктеуге, жүйеге командалар мен сұраныстарды енгізуге, деректер мен нәтижелердің графикалық көрінісін алуға және нәтижелерді сақтауға мүмкіндік береді.

Ақпаратты сақтаудың ішкі жүйесі жалпы деректер қорынан (ДҚ), модельдер қорынан (МҚ) және білім қорынан (БҚ) тұрады, олар оқу мәліметтерін, БЖ негізінде дайын модельдерді жинақтауға арналған.

Bayesian_Net ШҚҚЖ талдаудың негізгі ішкі жүйесі БЖ негізіндегі деректерді талдауға арналған. Яғни, ол БЖ және ықтималды қорытынды құруға, БЖ берілген құрылымы бойынша генерация жасауға және жасырын төбелердің параметрлерін оқытуды жүзеге асыруға мүмкіндік береді. Талдаудың негізгі ішкі жүйесі бес блоктан тұрады:

1 блок – деректермен жұмыс;

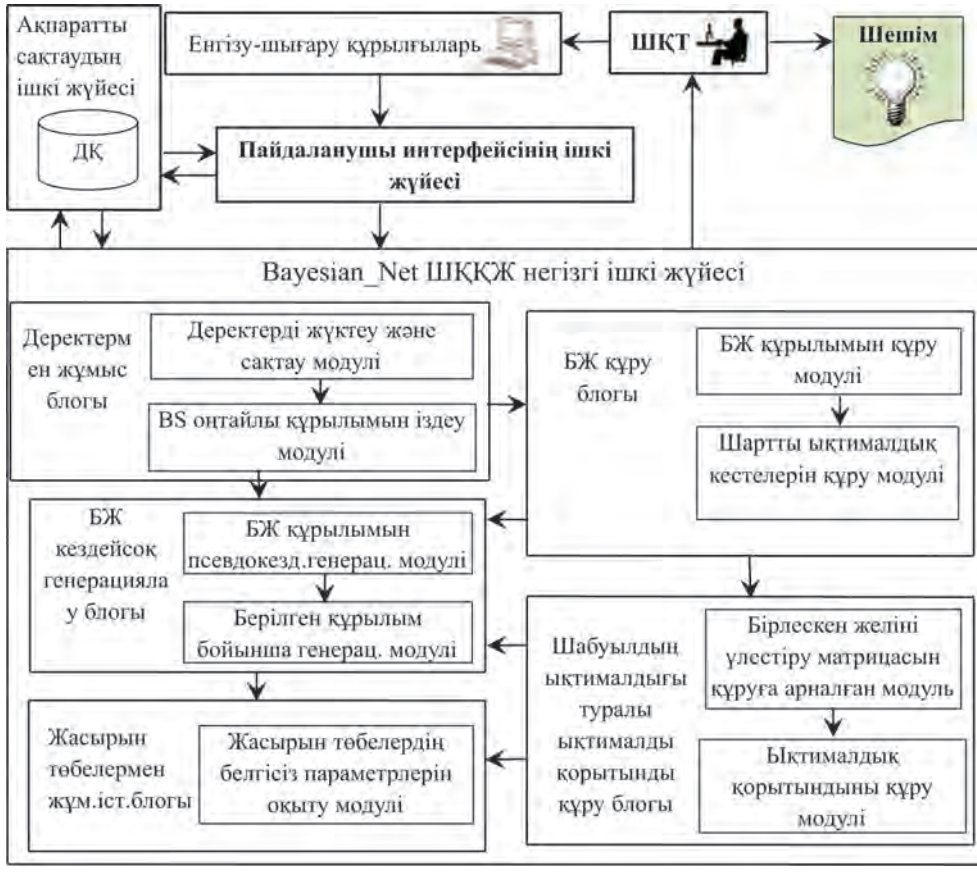
2 блок – БЖ құру;

3 блок – ықтималды қорытынды құру;

4 блок – кездейсоқ БЖ генерациясы;

5 блок – БЖ жасырын төбелерімен жұмыс істеу.

ШҚҚЖ Bayesian_Net-тің ішкі жүйесіне мәліметтер ақпаратты сақтаудың ішкі жүйесінен деректер шинасы арқылы келеді.



1 – сурет – Bayesian_Net ШҚҚЖ архитектурасы

Деректермен жұмыс істеу блогы БЖ оңтайлы құрылымын іздеуге, БЖ құру үшін сыртқы деректерді жүктеуге, сонымен қатар үлгіні генерациялау нәтижесінде алынған деректерді сақтау үшін арналған.

Бұл блок келесі модульдерден тұрады:

1 модуль – деректерді жүктеу және сақтау;

2 модуль – БЖ оңтайлы құрылымын іздеу.

Деректерді жүктеу және сақтау модулі деректерді Excel файлынан жүктеуге және жасалған деректерді Excel файлына қайта жазуға арналған.

БЖ-ның оңтайлы құрылымын іздеу модулі шыңдар арасындағы қатынасты есептеу әдісін таңдау арқылы желі топологиясын табу үшін БЖ құрудың эвристикалық алгоритмін қолданады.

Төбелер арасындағы өзара байланысты есептеуде келесі тәсілдер қолданылады: өзара ақпарат мәндері; Пирсон коэффициенті; Крамер коэффициенті; Чупров коэффициенті; Гудман лямбдасының мәні.

БЖ құру блогы графикалық интерфейсті қолдана отырып, БЖ-ны "қолмен" құруға мүмкіндік береді. Блок келесі модульдерден тұрады:

1 модуль – БЖ құрылымын құру;

2 модуль – шартты ықтималдық кестелерін құру.

БЖ құрылымын құру модулі БЖ-ны "қолмен" құруға арналған құралдарды қолданады және төбелерді, олардың арасындағы байланыстарды құруға және жоюға, төбелердің аттарын көрсетуге немесе жасыруға және құрылыс өрісін тазартуға мүмкіндік береді.

Шартты ықтималдық кестелерін құру модулі төбенің атын өңдеуге, төбенің күйін өзгертуге, оларды қосуға, өшіруге, атын өзгертуге және шартты ықтималдық кестелерін толтыруға мүмкіндік береді.

Ықтималдық қорытындыны құру блогы БЖ құрылымын құру блогынан келетін БЖ құрылымы бойынша ықтималдық қорытындысын құруға арналған. Блок келесі модульдерден тұрады:

1 модуль – бірлескен үлестіру матрицасын құру;

2 модуль – ықтималдық қорытындыны құру.

Бірлескен үлестіру матрицасын құруға арналған модуль барлық БЖ-ның бірлескен ықтималдық үлестірімінің эмпирикалық мәндерінің матрицасын құруға арналған.

Ықтималдық қорытындыны құру модулі ықтималдықтың бірлескен үлестірімінің эмпирикалық мәндерінің матрицасына негізделген БЖ-де ықтималдық қорытынды жасайды.

Кездейсоқ генерация блогы берілген параметрлер бойынша желі құрылымын псевдокездейсоқ генерациялауға және берілген құрылым бойынша іріктеуге арналған.

Блок құрамына келесі модульдер кіреді:

1 модуль – псевдокездейсоқ желі құрылымының генерациясы;

2 модуль – берілген құрылым бойынша іріктеменің генерациясы.

Желі құрылымын псевдокездейсоқ генерациялауға арналған модуль. БЖ-де аспалы төбелерді болдырмау үшін тізбектегі барлық төбелердің комбинациясы жүзеге асырылды. Бұл жағдайда байланыс бағыты кездейсоқ таңдалады. Салынған төбелер үшін байланыстар саны $N - 1$ болады. Онда $M - N + 1$ арқылы аталық пен еншілес төбелерін кездейсоқ таңдау арқылы салынған қалған байланыстардың санын өрнектейміз. Байланыс қосылған кезде циклдік тексеру жүргізіледі. Егер жаңа байланыс цикл құрса, онда ол қабылданбайды және БЖ үшін жаңа аталық мен еншілес төбелері таңдалады.

Шартты ықтималдық кестелері оларды 0-ден 1-ге дейінгі диапазондағы кездейсоқ сандармен толтыру арқылы анықталады, содан кейін қалыпқа келтіріледі (жол бойынша ықтималдық қосындыларын 1-ге келтіру қажет).

Берілген құрылым бойынша іріктемені генерациялау модулі. Іріктемені генерациялау келесідей болады. Алдымен, ықтималдық қорытынды БЖ-де анықталмаған (инстанцированных) төбелерсіз жасалады (төбелер үшін параметрлер берілмеген).

Әрі қарай, әр төбенің күйлері кезекпен өзгертіледі (класс даналары жасалады), олар іріктемедегі жазбалардың қажетті санын құрайды.

Жасырын төбелермен жұмыс істеу блогы жасырын төбелердің белгісіз параметрлерін оқытудың бір модулінен тұрады. Бұл блок логарифмдік ықтималдылық функциясының критерийі бойынша EM-алгоритмді пайдалана отырып, желі параметрлерін итерациялық табуға арналған.

Bayesian_Net ШҚҚЖ архитектурасының негізінде деректер мен анықталған ауытқулар туралы ӘҚД жағдайында кибершабуылдардың салдарын бағалау үшін БЖ қолдану негізінде деректерді талдауға арналған компьютерлік бағдарлама жүзеге асырылды. Іске асыру үшін Delphi 10 жоғары деңгейлі тілі (RAD Studio 10.4 жобалау ортасы) қолданылады. Rad Studio 10.4 жобалау ортасын таңдау себебі - ол тиімді объектіге бағытталған бағдарламалау құралы, дамыған алгоритмдерді ерекшеліктері мен әдістерді мұрагерлікпен класс иерархиясы түрінде ұсынуға мүмкіндік береді. Бұл ақпараттандырудың әртүрлі объектілерін одан әрі зерттеу үшін тиімді және сенімді бағдарламалық өнімді, икемді жүйені алуға мүмкіндік береді.

Bayesian_Net ШҚҚЖ келесі негізгі мүмкіндіктерді ұсынады:

Кез-келген тапсырмалар үшін, оның ішінде белгілер мен анықталған ауытқулар бойынша ӘҚД жағдайында кибершабуылдардың салдарын бағалау және деректерді талдау тапсырмалары үшін Байес желісінің құрылымын құру;

– АЖ КҚ-не анықталған ауытқулар мен белгілерді ӘҚД жағдайында кибершабуылдардың салдарын бағалау туралы ықтималды қорытынды қалыптастыру;

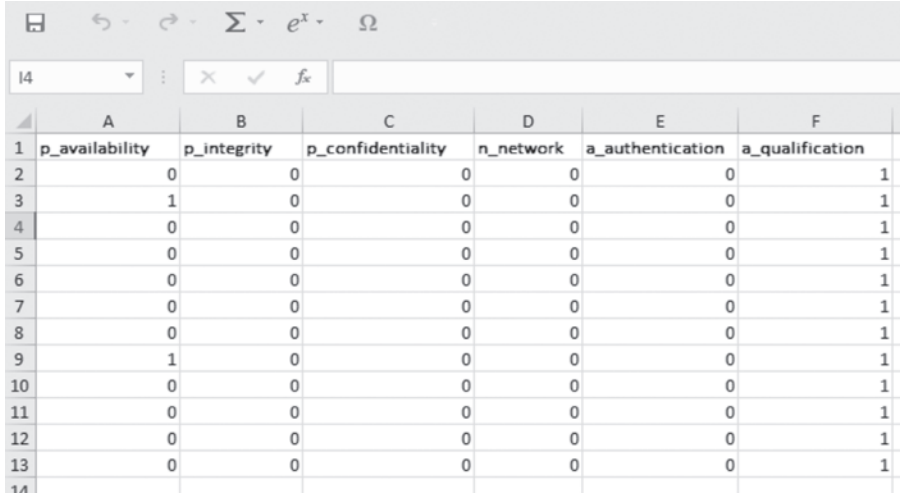
– БЖ құрылымы және іріктемелерді генерациялау;

– Жасырын төбелері бар белгісіз БЖ параметрлерін табу.

Bayesian_Net ШҚҚЖ пайдаланушыға ыңғайлы интерфейспен жасалған және оны игеру арнайы дағдыларды қажет етпейді. БЖ құру принциптері туралы жалпы білімнің болуы жеткілікті.

Bayesian_Net ШҚҚЖ ақпараттандыру объектісі желісіндегі белгілер мен анықталған ауытқулар туралы ӘҚД жағдайындағы кибершабуылдардың салдарын бағалау міндеттерін талдау процесінде сарапшысының көмегімен ақпараттық қауіпсіздікке байланысты мәселелерді шешуге бағытталған. Бастапқы кезеңде сарапшы қорғаныс объектісі үшін типтік жағдайлардың үлгілерін дербес жасай алады, яғни Bayesian_Net ШҚҚЖ -де тікелей БЖ құра алады немесе жоғарыда аталған мәселені шешуге арналған БЖ репозиторийін пайдалануға болады. Жалпы АО АКЖ-ге басып кірудің кезеңдері мен қауіптерін болжау кезінде ШҚҚЖ есептеу ядросы үшін жасалған БЖ үлгілері әмбебап болып табылады. Алайда, сарапшы өзінің қорғаныс объектісі үшін осы үлгілерді пайдалану ерекшеліктерін өз бетінше бағалауы керек. Бұрын [10, 11] жасалған жұмыстарда БЖ үлгілері көптеген кездейсоқ айнымалылармен жұмыс істеуге және кибернетикалық қауіптің немесе қорғаныс объектісінде берілген жағдайларда басып кірудің нақты кезеңінің ықтималдығын анықтауға мүмкіндік береді. ШҚҚЖ тиімді жұмыс істеу үшін репозиторийдегі БЖ-ны оқыту қажет. Bayesian_Net ШҚҚЖ-де БЖ оқытуда шартты қорғау объектісі үшін қолда бар статистикалық деректер негізінде Em-алгоритм қолданылды.

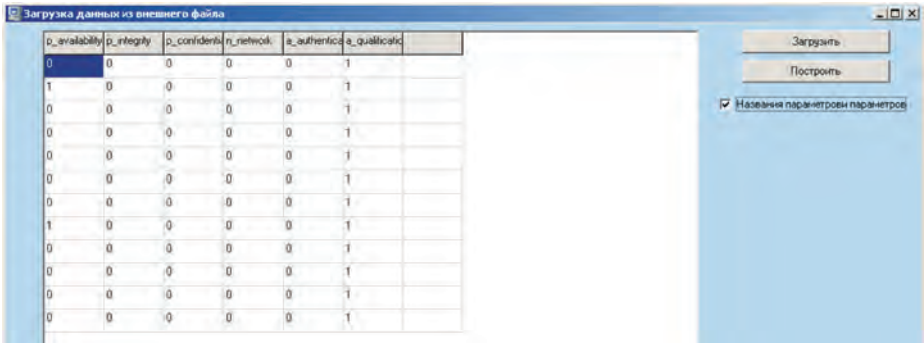
Сыртқы файлдан жүктелген деректер бойынша БЖ құру процесі қарастырылады. 2 және 3-суреттерде көрсетілгендей Bayesian_Net ШҚҚЖ Excel файлдарымен жұмыс істеуге арналған.



	A	B	C	D	E	F
1	p_availability	p_integrity	p_confidentiality	n_network	a_authentication	a_qualification
2	0	0	0	0	0	1
3	1	0	0	0	0	1
4	0	0	0	0	0	1
5	0	0	0	0	0	1
6	0	0	0	0	0	1
7	0	0	0	0	0	1
8	0	0	0	0	0	1
9	1	0	0	0	0	1
10	0	0	0	0	0	1
11	0	0	0	0	0	1
12	0	0	0	0	0	1
13	0	0	0	0	0	1

2 – сурет – Excel форматындағы деректердің мысалы

Excel файлындағы сыртқы деректердің мысалы ретінде "Ақпараттық жүйеде деректерді түрлендіру" қаупі үшін шартты ықтималдық кестесінің бөлігінің фрагменті келтірілген. Есептеу Bayesian_Net ШҚҚЖ-де ЕМ-алгоритмі бойынша жасалады.



3 – сурет – Excel файлынан жүктелген сыртқы деректер терезесінің мысалы

1-кесте – "Ақпараттық жүйеде деректерді түрлендіру" қаупінің шартты ықтималдық кестесі үшін эксперименталды түрде алынған мәндері (ЕМ-алгоритм бойынша есептеу)

Факторлар	p_availability	Толық					
	p_integrity	Толық					
	p_confidentiality	Толық					
	n_network	Сегментаралық					
	a_authentication	Болмау		Әлсіз			
	a_qualification	Төмен	Орташа	Жоғары	Төмен	Орташа	Жоғары

1-кестенің соңы

Қауіп деңгейі	trivial	0,00061	0,00061	0,027	0,0075	0,0075	0,027
	low	0,00061	0,00061	0,027	0,0075	0,0075	0,027
	medium	0,00061	0,00061	0,92	0,0075	0,0075	0,92
	high	0,999	0,999	0,027	0,99	0,99	0,027
	critical	0,00061	0,00061	0,027	0,0075	0,0075	0,027

Эксперименттік зерттеулер барысында белгілер мен анықталған ауытқулар туралы ӘҚД жағдайында кибершабуылдардың салдарын бағалау үшін БЖ пайдалану негізінде деректерді талдау тапсырмаларында Bayesian_Net ШҚҚЖ пайдалану мүмкіндігі расталды.

Қорытынды. Мақалада келесі нәтижелер алынды: БЖ негізінде деректерді талдау үшін әзірленген BAYESIAN_NET ШҚҚЖ архитектурасы сипатталды. Ұсынылған ШҚҚЖ объектіге бағытталған бағдарламалауды қолданумен ерекшеленеді және икемді модульдік архитектураға ие. Бұл мәселелер осы саладағы зерттеулерді жалғастыруда маңызды фактор және КҚ саласындағы шешім қабылдауды қолдауды интеллектуализациялаумен байланысты болып табылады. Алынған нәтижелер деректерді іздеу мәселелерін шешу үшін, атап айтқанда АО КҚ-мен байланысты әлсіз құрылымдалған мәселелерді талдау және белгілер мен анықталған ауытқулар туралы ӘҚД жағдайындағы кибершабуылдардың салдарын бағалау үшін Bayesian_Net ШҚҚЖ бағдарламалық өнімінің тиімділігін көрсетеді.

ӘДЕБИЕТ

1 Berik, A., Valeriy, L., Yuliia, B., & Andrii, M. (2017). Разработка системы поддержки решений в слабо формализуемых задачах обеспечения кибербезопасности. Восточно-Европейский журнал передовых технологий, 1(2 (85)).

2 Массель, А. Г., & Гаськова, Д. А. (2018). Методы и подходы к обеспечению кибербезопасности объектов цифровой энергетики. Энергетическая политика, (5), 62-72.

3 Авдошин, С. М., Лазаренко, А. В., Чичилева, Н. И., Наумов, П. А., & Ключарев, П. Г. (2019). Примеры использования машинного обучения в кибербезопасности. Труды Института системного программирования РАН, 31(5), 191-202.

4 Полтавцева, М. А., & Печенкин, А. И. (2017). Интеллектуальный анализ данных в системах поддержки принятия решений при тестировании на проникновение. Проблемы информационной безопасности. Компьютерные системы, (3), 62-69

5 Котенко, И. В. (2009). Интеллектуальные механизмы управления кибербезопасностью. Труды Института системного анализа Российской академии наук, 41, 74-103

6 Мирошник, М. А., Крылова, В. А., & Демичев, А. И. (2015). Применение интеллектуальной диагностической инфраструктуры для управления кибербезопасностью. Часть 1. Интеллектуализация механизмов защиты. Інформаційно-керуючі системи на залізничному транспорті, (6), 25-32.

7 Xie, P., Li, J. H., Ou, X., Liu, P., & Levy, R. (2010, June). Using Bayesian networks for cyber security analysis. In 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN) (pp. 211-220). IEEE.

8 Chockalingam, S., Pieters, W., Teixeira, A., & van Gelder, P. (2017, November). Bayesian network models in cyber security: a systematic review. In Nordic Conference on Secure IT Systems (pp. 105-122). Springer, Cham.

9 Полтавцева, М. А., & Печенкин, А. И. (2017). Интеллектуальный анализ данных в системах поддержки принятия решений при тестировании на проникновение. Проблемы информационной безопасности. Компьютерные системы, (3), 62-69

10 Lakhno, V., Akhmetov, B., Ydyryshbayeva, M., Bebeshko, B., Desiatko, A., & Khorolska, K. (2020, December). Models for Forming Knowledge Databases for Decision Support Systems for Recognizing Cyberattacks. In International Conference on Intelligent Computing & Optimization (pp. 463-475). Springer, Cham.

11 Akhmetov B.S., Lakhno V.A., Ydyryshbayeva M.B., Yagaliyeva B.E., Baiganova A.V., Akhanova M.B., Tashimova A.K. Application of bayesian networks in the decision support system during the analysis of cyber threats, Journal of Theoretical and Applied Information Technology, 99(4), pp. 884 - 893, 2021.

REFERENCES

1 Razrabotka sistemy podderzhki reshenij v slabo formalizuemyh zadachah obespecheniya kiberbezopasnosti. Vostochno-Evropejskij zhurnal peredovyh tekhnologij, 1(2 (85))]

2 Massel', A. G., & Gas'kova, D. A. (2018). Metody i podhody k obespecheniyu kiberbezopasnosti ob"ektov cifrovoj energetiki. Energeticheskaya politika, (5), 62-72.]

3 Avdoshin, S. M., Lazarenko, A. V., CHichileva, N. I., Naumov, P. A., & Klyucharev, P. G. (2019). Primery ispol'zovaniya mashinnogo obucheniya v kiberbezopasnosti. Trudy Instituta sistemnogo programmirovaniya RAN, 31(5), 191-202.]

4 Poltavceva, M. A., & Pechenkin, A. I. (2017). Intellektual'nyj analiz dannyh v sistemah podderzhki prinyatiya reshenij pri testirovanii na proniknovenie. Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy, (3), 62-69.]

5 Kotenko, I. V. (2009). Intellektual'nye mekhanizmy upravleniya kiberbezopasnost'yu. Trudy Instituta sistemnogo analiza Rossijskoj akademii nauk, 41, 74-103.]

6 Miroshnik, M. A., Krylova, V. A., & Demichev, A. I. (2015). Primenenie intellektual'noj diagnosticheskoj infrastruktury dlya upravleniya kiberbezopasnost'yu. CHast' 1. Intellektualizaciya mekhanizmov zashchity. Informacijno-keruyuchi sistemi na zaliznichnomu transporti, (6), 25-32.]

7 Xie, P., Li, J. H., Ou, X., Liu, P., & Levy, R. (2010, June). Using Bayesian networks for cyber security analysis. In 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN) (pp. 211-220). IEEE.

8 Chockalingam, S., Pieters, W., Teixeira, A., & van Gelder, P. (2017, November). Bayesian network models in cyber security: a systematic review. In Nordic Conference on Secure IT Systems (pp. 105-122). Springer, Cham.

9 Poltavceva, M. A., & Pechenkin, A. I. (2017). Intellektual'nyj analiz dannyh v sistemah podderzhki prinyatiya reshenij pri testirovanii na proniknovenie. Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy, (3), 62-69.]

10 Lakhno, V., Akhmetov, B., Ydyryshbayeva, M., Bebeshko, B., Desiatko, A., & Khorolska, K. (2020, December). Models for Forming Knowledge Databases for Decision Support Systems for Recognizing Cyberattacks. In International Conference on Intelligent Computing & Optimization (pp. 463-475). Springer, Cham.

11 Akhmetov B.S., Lakhno V.A., Ydyryshbayeva M.B., Yagaliyeva B.E., Baiganova A.V., Akhanova M.B., Tashimova A.K. Application of bayesian networks in the decision support system during the analysis of cyber threats, Journal of Theoretical and Applied Information Technology, 99(4), pp. 884 - 893, 2021.

Б. С. АХМЕТОВ[1], В. А. ЛАХНО[2] , М. Б. ЫДЫРЫШБАЕВА[3], А. К. АБУОВА[4], Ш. САГЫНДЫКОВА[5]

[1]Казахский национальный педогагический университет имени Абая, Алматы, Казахстан
[2]Национальный университет биоресурсов и природопользования, г. Киев, Украина.
[3]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
[4] Казахский университет путей сообщения, Алматы, Казахстан
[5]Алматинский университет энергетики и связи , Алматы, Казахстан
e-mail: bakhytzhan.akhmetov.54@mail.ru, valss21@ukr.net, moldir.ydyryshbaeva@gmail.com, abuova.akbala@mail.ru, Tomka2001@mail.ru

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ОЦЕНКИ ПОСЛЕДСТВИЙ КИБЕРАТАК

Описана архитектура системы поддержки принятия решений (СППР) Bayesian_Net, которая была разработана для анализа данных о признаках аномалий и кибератак на основе применения для этой задачи Байесовских сетей (БС). Предложенная СППР отличается применением объектно-ориентированного программирования и имеет модульную архитектуру. СППР Bayesian_Net предназначена для решения задач интеллектуального анализа данных, в частности для анализа слабоструктурированных проблем, связанных с кибернетической безопасностью (КБ) объектов информатизации (ОБИ), и оценки последствий кибератак в условиях слабо структурированных данных о признаках и выявленных аномалиях.

***Ключевые слова**: Баесовская сеть, кибернетическая безопасность, система поддержки принятия решений, программный продукт.*

B. S. AKHMETOV[1], V. A. LAKHNO[2], M. B. YDYRYSHBAYEVA[3], A. ABUOVA[4], SH. SAGYNDYKOVA[5]

[1]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan
[2] National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
[3]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[4]Kazakh University ways of Communications, Almaty, Kazakhstan
[5]Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
e-mail: bakhytzhan.akhmetov.54@mail.ru, valss21@ukr.net, moldir.ydyryshbaeva@gmail.com, abuova.akbala@mail.ru, Tomka2001@mail.ru

DECISION SUPPORT SYSTEM FOR ASSESSING THE CONSEQUENCES OF CYBER ATTACKS

The architecture of the Bayesian_Net decision support system (DSS) is described, which was developed to analyze data on signs of anomalies and cyberattacks based on the use of Bayesian Networks (BN) for this task. The proposed DSS is distinguished by the use of object-oriented programming and has a modular architecture. The Bayesian_Net DSS is designed to solve data mining problems, in particular, to analyze weakly structured problems related to cybernetic security (CS) of informatization objects (IO), and to assess the consequences of cyber attacks in conditions of weakly structured data on signs and detected anomalies.

***Keywords**: Bayesian network, cybernetic security, decision support system, software product.*