МРНТИ 50.47
УДК 004.056

https://doi.org/10.51889/2959-5894.2023.81.1.021

М.Б. Ыдырышбаева[1], Б.С. Ахметов[2]*

[1]әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы қ., Қазақстан
[2]Абай атындағы Қазақ Ұлттық Педагогикалық Университеті, Алматы қ., Қазақстан
[*]e-mail: moldir_ydyryshbaeva@gmail.com

КИБЕРҚАУІПСІЗДІКТЕ ШЕШІМДЕРДІ ҚАБЫЛДАУДЫ ҚОЛДАУ ЖҮЙЕСІНДЕГІ МЕТАБІЛІМДІ СИПАТТАУ МОДЕЛІ

Аңдатпа

Мақалада ақпараттандыру объектілерінде (АО) кибер қауіпсіздікті (КҚ) қамтамасыз ету міндеттерінде қолданылатын шешімдерді қабылдауды қолдау жүйелерінің (ШҚҚЖ) тұжырымдамасы ұсынылған. АО киберқорғау процестерін түсінуді арттыруға мүмкіндік беретін аномалиялар мен шабуылдардың жеке түсіндіруге қиын белгілерін анықтауға байланысты жағдайлар үшін ШҚҚЖ білім базасын (ББ) қалыптастыру және қолдану процесінің тұжырымдамалық және функционалдық аспектісінде ұсыну моделі сипатталған. Әзірленген үлгі модельдер әртүрлі кезеңдерде әлсіз құрылымдық белгілермен сипатталуы мүмкін басып кіруді анықтау кезінде ШҚҚЖ есептеу ядросын құрайды. Маңызды ғылыми-техникалық міндет АО қауіпсіздігіне кибернетикалық қауіптер деңгейінің артуымен, КҚ-ға қойылатын талаптардың бір мезгілде артуымен сыртқы зиянды әсер ету қарқындылығының артуы арасындағы айқын қарама-қайшылыққа сүйене отырып, ақпараттық жүйелердегі (АЖ) белгілер мен анықталған ауытқулар туралы әлсіз құрылымдалған деректер жағдайында интеллектуалды ШҚҚЖ арналған әдістер мен модельдерді одан әрі дамыту және жаңа әдістер мен модельдерді әзірлеу болып табылады.

Түйін сөздер: шешім қабылдауды қолдау жүйелері, басып кіруді анықтау, модельдер, ақпараттық ресурстар.

Аннотация

М.Б. Ыдырышбаева[1], Б.С. Ахметов[2]

[1]Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан
[2]Казахский национальный педагогический университет имени Абая, г. Алматы, Казахстан

МОДЕЛЬ ОПИСАНИЯ МЕТАЗНАНИЙ В СИСТЕМЕ ПОДДЕРЖКИ РЕШЕНИЙ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

В статье представлена концепция систем поддержки принятия решений (СППР), применяемых в задачах обеспечения кибербезопасности (КБ) на объектах информатизации (ОБИ). Описана модель представления в концептуальном и функциональном аспекте процесса формирования и применения базы знаний (БЗ) СППР для ситуаций, связанных с выявлением трудноизъяснимых признаков аномалий и атак, позволяющая повысить понимание процессов киберзащиты на ОИБ. Разработанный шаблон и модели составляют вычислительное ядро СППР в ходе выявления вторжений, которые могут на разных этапах характеризоваться слабоструктурированными признаками. Исходя из существующего явного противоречия между увеличением уровня кибернетических угроз безопасности ОБИ и повышением интенсивности внешних вредоносных воздействий с одновременным повышением требований к КБ, важной научно-технической задачей является дальнейшее развитие существующих и разработка новых методов и моделей для интеллектуальных СППР в условиях слабо структурированных данных о признаках и выявленных аномалиях в информационных системах.

Ключевые слова: системы поддержки принятия решений, обнаружение вторжений, модели, информационные ресурсы.

Abstract

A MODEL FOR DESCRIBING META-KNOWLEDGE IN A CYBERSECURITY SOLUTION SUPPORT SYSTEM

Ydyryshbayeva M.B.[1], Akhmetov B.S.[2]

[1]Al Farabi Kazakh National University, Almaty, Kazakhstan
[2]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan

The article presents the concept of decision support systems (DSS) used in cybersecurity (CS) tasks at at objects of informatization (OI). The paper describes a model of representation in the conceptual and functional aspect of the process of forming and applying the knowledge base (KB) of the DSS for situations involving the identification of difficult-to-

explain signs of anomalies and attacks, which allows to increase the understanding of cyber defense processes at the OI. The developed template and models make up the computational core of the DSS during the detection of intrusions, which may be characterized by weakly structured features at different stages. Based on the existing apparent contradiction between an increase in the level of cybernetic threats to the security of the OI and an increase in the intensity of external malicious influences with a simultaneous increase in requirements for CS, an important scientific and technical task is to further develop existing and develop new methods and models for intelligent DSS in conditions of poorly structured data on signs and identified anomalies in information systems.

Keywords: decision support systems, intrusion detection, models, information resources.

1. Кіріспе

Кибернетикалық қауіптер мен инциденттердің көбеюінің тұрақты тенденциясы, шабуылдардың күрделілігінің артуы және хакерлердің компаниялар мен ұйымдардың ақпараттық ресурстарына (АР) рұқсатсыз қол жеткізудің алуан түрлі әдістерін пайдалануы жағдайында, басып кіруді анықтау жүйелерінің (БКАЖ) рөлі артып келеді. Аталған мәселелерді шешуде ақпаратты қорғаудың интеллектуалды жүйелері ақпараттық қауіпсіздік құралдарын (АҚҚ) қолданылады. Қорғаныс тарабы күрделі жағдайларды түсіндірумен байланысты нақты міндеттерді интеллектуалды ақпараттық қауіпсіздік жүйелеріне (АҚЖ) жүктейді. Мұндай жағдайлар үшін шабуыл белгілері айқын емес және шабуылдардың әлсіз құрылымдалған белгілерін терең талдауды және оларды жүзеге асырудың ықтимал салдарын талап етеді. АҚЖ БКАЖ интеграциясы көптеген заманауи шабуылдардың алдын алуға мүмкіндік береді [1].

Сонымен қатар, ақпараттық жүйелер (АЖ) және ақпараттық технологиялар (АТ) компанияларының бизнес процестеріне терең интеграциялау ақпараттандыру объектілері үшін кибернетикалық қауіптердің санын ұлғайтты. Сондықтан компаниялардың қалыпты жұмыс істеуін қамтамасыз ету, олардың АЖ және басып кіруді болдырмау үшін қатерлерді жою бойынша адекватты ұйымдастырушылық және техникалық шаралар қажет. Ең алдымен, кибернетикалық шабуылдар сценарийлерінің күрделілігінің өсуі жағдайында арнайы кибернетикалық қауіпсіздік құралдарына (КҚ) назар аудару керек.

Соңғы онжылдықта ақпараттық және кибернетикалық қауіпсіздік саласында белсенді дамып келе жатқан өзекті бағыттардың бірі кибершабуылдарды анықтау және авторланбаған торап тарапынан ақпараттандыру объектілерінің (АО) ақпараттық жүйелеріне (АЖ) басып кіруді болдырмау болып табылады.

Жаппай (массированные) кибернетикалық шабуылдар ақпараттық қауіпсіздік және киберқауіпсіздіктің әртүрлі ақпараттандыру объектілерін қамтамасыз ету саласындағы инновациялық зерттеулердің тұтас толқынын тудырды. Сондай – ақ, шабуылдарға қарсы арнайы техникалық шешімдер, құралдар мен жүйелерді әзірлеуге және жасауға бастамашылық етті. Бүгінгі таңда желілік шабуылдарды анықтау үшін КҚ мамандары заманауи әдістердің, модельдердің, құралдардың, бағдарламалық жасақтаманың (БҚ) барлық арсеналын қолданады. Кешенді техникалық шешімдер кеңінен қолданыла бастады. Бұл кешенді шешімдер басып кіруді анықтау (БКАЖ) және алдын алу жүйелерін қамтиды. АҚЖ БКАЖ интеграциясы көптеген заманауи шабуылдардың алдын алуға мүмкіндік береді. Инновациялық БКАЖ киберқауіптер мен шабуылдардың жаңа немесе модификацияланған түрлері пайда болған кезде тиімді жұмыс істей алады.

Ақпаратты қорғау теориясының қазіргі заманғы даму тенденциялары, сондай-ақ, басып кіруді (кибернетикалық шабуылдарды) анықтау процесін интеллектуалдандырумен байланысты қолданбалы міндеттер үлкен көлемдегі деректерді талдаудың көптеген мәселелерін шешуді, олардағы заңдылықтар мен қатынастарды табуды қажет етеді. Көбінесе, АҚ және КҚ АО қамтамасыз етумен байланысты мұндай міндеттер, белгісіздіктің әртүрлі жағдайдағы шарттарымен сипатталады. Сондай-ақ, мұндай міндеттер толық емес, анық емес ақпараттың болуымен сипатталады және адам факторының әсерінен оларды шешу қиындайды. Сондықтан мұндай әлсіз құрылымдалған мәселелерді шешу өте маңызды.

Қаскүнемнің қауіптерін жүзеге асыру ықтималдығын бағалау сапасын арттыру үшін шешім қабылдауды қолдаудың интеллектуалды жүйелерін (ШҚҚЖ) АҚҚ-ға интеграциялау арқылы ақпараттандыру объектілерінің АР қорғалу дәрежесін арттыру жұмыстың өзектілігі болып табылады [2].

2. Әдебиеттерге шолу және талдау

Қазіргі қоғам сандық экономиканың көптеген салаларында шешуші рөл атқаратын ақпараттық технологияның (АТ) барлық артықшылықтарын пайдаланады. Бұл жағдайда киберқауіпсіздіктің (КҚ)

қоғам үшін маңызы өте зор болып отырғаны анық. Бүгінгі таңда киберқауіпсіздік және киберқауіпсіздік мәселелері осы саланың мамандарын ғана алаңдатпайды. КҚ саласындағы оқиғалар ақпараттық және басқа да көптеген қызметтерді тұтынушылардың өміріне әсер етеді. Кибершабуылдардың ауыр техникалық-экономикалық салдары да, олардың саны мен әртүрлілігінің өсу тенденциясы да үлкен алаңдаушылық тудырады, бұл статистикалық есептілікте және жетекші әлемдік компаниялардың киберқауіпсіздік КҚ бойынша тиісті шолуларында көрінеді. Жаппай кибернетикалық шабуылдар АҚ және КҚ әртүрлі ақпараттандыру объектілерін (АО) қамтамасыз ету саласындағы инновациялық зерттеулердің тұтас толқынын тудырды. Сонымен қатар, олар арнайы техникалық шешімдер - шабуылдарға қарсы тұру құралдары мен жүйелерін жасау мен құруға бастамашы болды. Желілік басып кіруді анықтау үшін КҚ мамандары қазіргі заманғы әдістердің, модельдердің, құралдардың, бағдарламалық жасақтамалардың (БЖ) толық арсеналын қолданады. Кешенді техникалық шешімдер де кеңінен қолданыла бастады. Сонымен қатар, бұл шешімдердің ажырамас бөлігі ретінде басып кіруді анықтау жүйесі (БКАЖ) және БКАЖ болдырмау жүйесін қамтиды. БКАЖ қолдану қазіргі заманғы шабуылдардың көпшілігін болдырмауға мүмкіндік береді және киберқауіптер мен шабуылдардың жаңа немесе түрлендірілген түрлері пайда болған кезде айтарлықтай тиімді жұмыс істей алады. Шабуылдар туралы деректер немесе аномалиялар әлсіз құрылымдалған жағдайда БКАЖ өзгертілген бастапқы деректерге сәйкес бейімдеу үшін ұзақ уақыт қажет. Сондықтан, БКАЖ үнемі жетілдірілуі керек, олардың тиімді жұмыс істеуінің үздіксіздігін қамтамасыз ету үшін қажет. Қазіргі заманғы БКАЖ арасында олардың дамуының бірнеше бағыттарын бөлуге болады. Ең алдымен, КҚ құралдарының осы класына мамандандырылған бағдарламалық құралдарды (МБҚ) жатқызуға болады. Мұндай МБҚ әрекеті АЖ немесе АО желісіндегі күдікті әрекеттерді анықтауға бағытталған. Сондай-ақ, мұндай МБҚ АЖ және АО компьютерлік желілерінің жұмысына араласу әрекеттерін анықтауға және құжаттауға көмектеседі [3].

Киберкеңістікті құрайтын элементтердің саны, олардың арасындағы өзара байланыстар, осы элементтерді басқарудың арнайы әдістерін қолдану мүмкіндігі алдағы онжылдықта жаһандық киберкеңістікте үстемдік ете алатын қауіптердің жаңа көрінісін дамыту мүмкіндіктерін анықтайды. Киберкеңістікте уақыт өткен сайын мамандар болжағандай күрделі қауіптер дамуы мүмкін. Бұл қауіптер мен шабуылдарды жан-жақты талдау және осы талдаудың нәтижелерін пайдалану, оның ішінде қолданыстағы және болашақта киберқауіптер мен шабуылдарға тиімді қарсы тұру үшін шешім қабылдауды қолдаудың интеллектуалды технологияларын қолдану міндетін өзекті етеді. АО қауіпсіздігіне кибернетикалық қауіптер деңгейінің артуы мен КҚ-ке қойылатын талаптардың бір мезгілде артуымен сыртқы зиянды әсерлердің қарқындылығының артуы арасындағы қазіргі қарама-қайшылыққа сүйене отырып, маңызды ғылыми-техникалық міндет АЖ-да белгілер мен анықталған ауытқулар туралы әлсіз құрылымдалған деректер жағдайында шешімдер қабылдауды қолдаудың интеллектуалдық жүйелері үшін бар әдістер мен модельдерді одан әрі дамыту және жаңа әдістер мен модельдерді әзірлеу қажет [4].

Киберқауіптер мен кибернетикалық инциденттердің өсуінің тұрақты тенденциясы жағдайында, шабуылдардың күрделілігінің артуы, хакерлердің компаниялар мен ұйымдардың ақпараттық ресурстарына рұқсат етілмеген қолжетімділіктің алуан түрлі техникаларын қолдануы, интеллектуалды анықтау технологияларының, сондай-ақ интеллектуалды ақпаратты қорғау жүйесінің рөлі артуда. Сонымен қатар, шабуыл белгілері айқын болмаған және шабуылдардың жиі әлсіз құрылымдалған белгілерін және оларды жүзеге асырудың ықтимал салдарын тереңірек талдауды қажет ететін күрделі жағдайларды түсіндіруге байланысты нақты міндеттер жүктелген. Кибершабуылдардың даму тенденциялары жылдан жылға өзгеріп отырады. Кибершабуылдарды дайындау мен өткізудің заңдылықтарын зерттеу және олардың арасындағы байланысты анықтау және шабуылдардың нысандарына әртүрлі факторлардың әсерін анықтау үшін деректерді талдаудың интеллектуалды технологиялары мен шешімдерді қолдау жүйелерінің мүмкіндіктерін кеңірек пайдалану қажет. Соңғы жылдары АО-де кибершабуылдардың көбеюі тиімді АҚЖ-ны дамытуға қызығушылық тудырды. Осы саладағы зерттеулердің перспективалы және жеткілікті жаңа бағыты АҚ саласындағы ШҚҚЖ және сараптамалық жүйелердің (СЖ) әдістерін, модельдерін және бағдарламалық кешендерін дамыту бойынша жұмыстар болды [5].

БКАЖ және ШҚҚЖ негізінде адаптивті киберқорғаныс (АКҚ) тетіктерін іске асыратын аппараттық-бағдарламалық кешендер әлі де қалыптасу сатысында. [6] еңбек киберқауіпсіздікте белгілер мен анықталған аномалиялар туралы әлсіз құрылымдалған деректер жағдайында кибершабуылдардың салдарын бағалау үшін шешімдерді қабылдауды қолдау жүйесінде метабілімді

сипаттау моделін дамытуға арналған. Ақпараттық-коммуникациялық жүйелерде аномалияларды, шабуылдарды және қауіптерді анықтау процесінде қолданылатын әдістер мен алгоритмдерге жүргізілген зерттеулер ақпаратты қорғау саласында ШҚҚЖ модельдерін дамытуды көздейді [7].

3. Зерттеудің мақсаты – әлсіз құрылымдалған деректер жағдайында анықталған ауытқулар белгілері мен кибершабуылдар салдарын бағалауға арналған шешім қабылдауды қолдау жүйесіндегі метабілімді сипаттау моделін әзірлеу.

4. Модельдер мен әдістер

БКАЖ және ШҚҚЖ негізінде адаптивті киберқорғаныс (АКҚ) тетіктерін іске асыратын аппараттық-бағдарламалық кешендер әлі де қалыптасу сатысында болғандықтан, оларды әзірлеуге арналған формализацияланған есептер келесі түрде тұжырымдалған.

Мұндай БКАЖ үшін бастапқы деректер ББ (білім базасы) құрамындағы – REP деректер болады:

$$REP = \langle SYS, Events, TAI, NIS, gov \rangle, \quad (1)$$

Мұндағы, SYS – АҚО инфрақұрылымы туралы деректер (мысалы, топология, пайдаланушылар, қорғау құралдары мен әдістері және т. б.);

$Events$ – БКАЖ-мен тіркелген оқиғалар;

TAI – үлгілер (сценарии);

NIS – шабуылдарға қарсы үлгілер;

gov – шабуылдарды анықтауда шешуші ережелер [14].

БКАЖ компоненті ретінде ШҚҚЖ шешетін есептер келесідей анықталған.

АҚО қауіпсіздігін талдау:

$$IOFP_j = FS(SYS, TAI, AT, gov), \quad (2)$$

Мұндағы, АҚО қауіпсіздігінің $IOFP_j$ – j -ші көрсеткіші;

AT – КҚ-ны бұзумен байланысты оқиғалар;

FS – қауіпсіздік саясатымен анықталған функция.

Шабуылды жүзеге асыру процесінде жағдайдың өзгеруін модельдеу:

$$ESC_{cr} = Model(SYS, TAI, AT, gov, T), \quad (3)$$

Мұндағы, $ESC_{cr} \subset SYS$ – АҚО сыни (критичный) элементі;

$Model$ – T уақыт бойынша кибершабуыл моделі.

Шабуылдарға қарсы тұруға арналған шешімдерді қолдау, атап айтқанда, ақпаратты қорғаудың әлсіз формализацияланған еептері үшін:

$$CM = \arg \min \left| IOFP - IOFP_{\text{rt}} \right|, \quad (4)$$

Мұндағы, $CM \subset gov$ – қарсы шаралар (контрмеры);

$IOFP$, $IOFP_{\text{r}}$ – тиісінше, АҚО қорғалу көрсеткішінің ағымдағы және эталондық мәні,

5. Есептеу эксперименттері

ШҚҚЖ-де АҚ (немесе КҚ) қамтамасыз ету жөніндегі шешімді қолдау есебімен байланысты жағдайды құрылымдау рәсімі функционалдық және құрылымдық мәнмәтіндерде (контекст) қаралды.

Құрылымдық тәсілдің нұсқасы жағдайды декомпозициялауға мүмкіндік береді. Бұл оның (se_i) құрамдас бөліктерінің құрылымдық-функционалдық қатынастарын талдауға мүмкіндік береді. БКАЖ және ШҚҚЖ негізделген [8, б. 7-11] және иерархиялық компонентпен «Бөлік-бүтін (Часть-Целое)» ұсынылған (se_i) компонентін іріктеу,

$$\langle PA, WH \rangle, \quad (5)$$

мұндағы, $PA = \{pa_i\}$ – бүтін (жиынтық немесе алфавит (se_i));

$WH - PA, i = 1,..., n$ алфавиттегі «Бөлік-бүтін» қатынасы.

Функционалды тәсілдің нұсқасы үшін жағдайды анықтау (дефиниция) АҚО жұмысына заңсыз араласудың базистік бағаларын анықтайды.

$SI_i = \{si_{ij}\}$, жағдайдың барлық компоненттері үшін қабылданады, $j = 1,..., m$ – төбелердің жиынтығы, (pa_i) жағдайдың әр компоненті (se_i) үшін оның функционалды құрылымын анықтайтын AM_i – бағытталған графтың (БГ) сыбайластық матрицасы (СМ).

Сарапшылардың білімі мен біліктілігін қолдана отырып, АҚҚе қорғаныс жүйесі элементінің жұмыс істеу заңдылықтарын субъективті түсіндіруді көрсететін когнитивтік карталарды (КОГК) (SI_i, AM_i) құрамыз.

Содан кейін алынған КОГК (SI, AM) топтастырылады, мұндағы, $SI = \cup SI_i$ жағдайдың өзгеруін сипаттайтын («Б») белгілер жиынтығы.

Әзірленген ШҚҚЖ-де білімді бейнелеу моделі белгілі БГ түрінде, сондай-ақ білім өрісі (БӨ) қолданылады [8, б.12].

БӨ ШҚҚЖ есептері үшін кіріс деректерімен (X – факторлар); қорытындылармен (Y – шығыс деректер); бастапқы деректерді шығысқа түрлендіру үшін пайдаланылатын модельдермен (МО) белгіленеді.

Модель жалпы түрде SC_{pa}, FS_{si} жүйелермен сипатталған. SC_{pa} және FS_{si} жүйелер, сәйкесінше, жағдайдың құрылымын және АҚҚе қауіпсіздік саясатын (ҚС) жүзеге асырудың заңдылықтарын көрсетеді.

КОГК (SI, AM) БӨ функционалды жүйесінде (ФЖ) сипатталған. КОГК сипаттау барысында белгілердің ақпараттылық шкаласы қолданылды [9, б.347; 10, б. 139]. Сонымен қатар, КОГК-ны сипаттау үшін жағдайды өзгерту сценарийлерін (pa_i) талдайтын сарапшының (шешім қабылдаушы тұлға -ШҚТ) қалауын анықтау әдістері қолданылды.

[10, б. 140] жағдайды трансформациялау сценарийін алу қажет жағдай үшін бастапқы деректер мыналар болып табылады: $SI = \{si_i\}$ факторларының жиынтығы; X_{ij} факторлардың шкаласы (шкалалар); талданатын жағдай туындағанға дейінгі АО бастапқы күйі:

$$X(t_0) = (x_{11},..., x_{nm}); \quad (6)$$

$$\text{СМ } AM = \left|am_{ij\,sl}\right|, \quad (7)$$

мұндағы, i, s – ұғым нөмірі;

Тиісінше, $i \vee s$ нөмірлерімен j, l – пайымдау белгісінің нөмірі.

Жалпы жағдайда $t,..., t+n$ мезеті үшін $X(t), X(t+1),..., X(t+n)$ кіріс параметрлерінің АО күйінің өзгеруін бақылау және белгілерді қосу векторын (БҚВ) анықтау қажет $V(t), V(t+1),..., V(t+n)$.

Мәселені шешу үшін реттелген итерация әдісі (метод последовательных итераций) қолданылды, оның барысында өрнектен БҚВ анықталды:

$$V(t+1) = V(t) \circ AM . \quad (8)$$

$t+1$ мезетіндегі АО жағдайы, $X(t+1) = X(t) + V(t+1)$ қатынасымен сипатталады.

БМ жолдарында – t уақыт мезетіне белгілерді қосу, бағанға сәйкес келетін бағанға уақыт мезетіне белгілерді қосу:

$$V^t = \left|V'(t+1)^T,..., P'(t+n)^T\right|. \quad (9)$$

V^t блоктық матрица КҚ АҚ жағдайдың өзгеруін (трансформация) болжаудың ішкі жүйесінде ШҚҚЖ-да қолданылды.

[11, б. 62] жұмыстарда көрсетілгендей БӨ элементтерінің сәйкес келмеу дәрежесі – $dis_{ij}(t)$, төмендегі өрнекпен анықталады:

$$dis_{ij}(t)=\frac{\left|v_{ij}^{+}(t)-v_{ij}^{-}(t)\right|}{v_{ij}^{+}(t)+v_{ij}^{-}(t)},\ 0\le v_{ij}(t)\le 1, \tag{10}$$

$D_{\max}$ және $D_{\min}$ үшін кері есепті шешудің қорытындылар нұсқалары [12, б. 172] жұмыстарда көрсетілген. D_i бақылау әсерлері, si_{ij} белгілерге v_{ij} және dis_{ij} параметрлері, сонымен қатар $D=\left(v_{11},dis_{11},...,v_{nm},dis_{nm}\right)$ арқылы орнатылады. Сәйкесінше, ШҚҚЖ-дағы dis_{ij} және v_{ij} параметрлері (12) және (13) қатынастарының көмегімен анықталады.

БӨ функционалдық жүйесінің (ФЖ) ағымдағы күйі $\langle SI,\ X,\ X(0),\ AM\rangle$ кортежбен айқындалған.

ШҚҚЖ құрамындағы БӨ (ҰЖ) ұғымдық жүйесі жағдайдың $\langle PA, WH\rangle$ құрылымдық-функционалдық декомпозициясын орындауға мүмкіндік береді. Сонымен қатар, ол жағдайды өзгерту сценарийлеріне қатысты қорытындыларды түсіндіру процестерінде, мысалы, мақсатты кибершабуылдарды жүзеге асыру кезінде қолданылады.

ШҚҚЖ-де жағдайдың компоненттері келесі параметрлермен анықталады

$$\langle pa_i, SI(pa_i), CV(pa_i)\rangle, \tag{11}$$

Мұндағы, pa_i – ұғым идентификаторы; $SI(pa_i)$ – ұғым интенциясы $SI_i=\{si_{ij}\}, SI(pa_i)=(x_{11},...,x_{nm})$); $CV(pa_i)$ – ұғымды қамту (модельде сипатталған жағдайдың компоненттері).

ШҚҚЖ-де pa_i ұғымы кеңістікте ұғымдар белгілерінің мәндерінің координаталары $(x_{11},...,x_{nm})$ нүктелер арқылы көрсетіледі.

Ұғымдар белгілерінің кеңістігі барлық белгілердің шкалаларының декарттық көбейтіндісімен қалыптасады – $U(pa_i)$.

ҰЖ моделінде $pa_i\in PA$ ұғым идентификаторы $U(pa_i)$ мағыналық кеңістігінде (семантикалық [13, б. 97]) көрсетілген. ҰЖ семантикалық кеңістік жиынын $U(PA)=\{U(pa_1),...,U(pa_n)\}$ және иерархиялық компонентті WH («Бөлік-бүтін») анықтауға мүмкіндік береді

Осылайша, $U(pa_i)$ және $U(pa_q)$ ұғым жұбы WH қатынасымен байланысты, сонымен қатар, $U(pa_i)\ WH\ U(pa_q)$.

КҚ саласында әзірленген ШҚҚЖ үшін CL^{i} [14, б. 310-312] өкілдік (представительный) кластерлер форматында pa_i негізгі ұғымдар үшін мағыналық кеңістікті құрылымдау жүргізілді. Кластерлер мен ұғымдар "Кластар-Ішкі кластар" қатынастарымен байланысты.

ШҚҚЖ-да, егер $\left(SI\left(pa_i^1\right)\subset SI\left(pa_i^2\right)\right)$ және $\left(CV\left(pa_i^1\right)\supset CV\left(pa_i^2\right)\right)$ шарттары орындалса pa_i^1 класы pa_i^2 класын көрсететіндігі қабылданады.

АҚ мағыналық кеңістігіндегі ұғымдық кластерлер pa_i^B базистік ұғымдарды (БҰ) түсіндіруде (трактовка) анықталған.

БҰ БКАЖ және ШҚҚЖ көмегімен талданатын объектілер класын (мысалы, шабуыл класы) және pa элемент жатқызылған жағдайдың санатын (категория) анықтайды.

Сараптамалық жолмен КШИТЖ (кибершабуылдарды интеллектуалды тану жүйесі) және ШҚҚЖ қарастыратын объектілер кластарының шекараларын анықтайтын $X_{ij}^{B}=\left[x_{ijb},x_{ijc}\right],\ \ x_{ij}\in X_{ij}^{B},\ \ \forall j$ мәндер аралығы белгіленеді.

ҚС терминдерінің кеңістігіне жататын АҚ-тің мағыналық (семантикалық) ұғымдары шеңберінде, сонымен қатар $U(pa^o) \subseteq U(cv^0)$, si_{ij} белгі үшін $U(pa^o)$ рұқсат етілген мағыналық мән салалары болады, мысалы осалдықтар табылды, ішінара табылды, табылмады және т. б.

БҰ параметрлермен анықталады:

$$\left(pa_i^B, SI\left(pa_i^B\right), CV\left(pa_i^B\right)\right), \tag{12}$$

Мұндағы, pa_i^B – БҰ идентификаторы;

$SI\left(pa_i^B\right)$ – БҰ интенциясы;

$CV\left(pa_i^B\right)$ – БҰ қамту (охват).

БҰ қамту белгілердің мәндері қолайлы болып табылатын ҚС объектілерінің жиыны ретінде ұсынылуы мүмкін. Ақпараттық қауіпсіздікті талдау (АҚТ) тұрғысынан қолайлы мәндер рұқсат етілген БҰ $AC(pa_i^B)$ параметрлері аймағына жатады.

БҰ жалпылау (генерализация) процедурасы қайталанатын белгілерді немесе олардың комбинацияларын жою арқылы жүзеге асырылады.

АҚ-ға арналған БҰ-да m саны бар абстракциялар $A = 2^m - 1$ қабылданды.

АҚ алфавитінің жалпыланған ұғымдарының рұқсат етілген мәндеріне БҰ мәндері енгізілген.

Осылайша, $AC\left(pa_i^B\right) \subset AC\left(pa_i^{Ba}\right)$ и $CV\left(pa_i^B\right) \subset CV\left(pa_i^{Ba}\right)$.

БҰ интенциясы және оның абстракциялары $\left\{SI\left(pa_i^B\right), SI\left(pa_i^{B1}\right), ..., SI\left(pa_i^{BA}\right)\right\}$ ішінара реттелген жиынтықты құрайды. Құрылған жиын ұғымдық кластер (ҰКЛ) БҰ - PA^i көрсетеді. Құрылған ҰКЛ КҚ мағыналық кеңістігін құрылымдауға мүмкіндік береді. Кластерлерде БҰ pa_i^B-дан жалпыланған pa_i^{Ba} дейін ауысулар анықталады. ҰЖ шеңберінде ШҚҚЖ-да ауысулар векторлар кортежімен беріледі:

$$\left\langle CN(t), CC(t), SV(t)\right\rangle, \tag{13}$$

6. Есептеу экспериментінің нәтижелерін талқылау

ШҚҚЖ жұмыс істеу процесінде БӨ ҰЖ трансформациялау ережелері айқындалды. Абстрактілі ережелер келесідей тұжырымдалған:

1) егер кибершабуылдың даму нәтижелерін болжау кезінде тұжырымдама белгісінің мәні БҰ рұқсат еткен шегінен асып кетсе, жаңа тұжырымдама қалыптасады;

2) жаңа ұғымдар бастапқы БҰ мәндері рұқсат етілгеннен ауытқитын белгілері бойынша жинақтайды.

Ресми түрде, ережелер ФЖ $X(T)$ күйін ҰЖ күйіне көрсету ретінде ұсынылады, яғни:

$$\begin{aligned}&\left\langle CN(t), CC(t), SV(t)\right\rangle, UM : X(t) \rightarrow \\ &\rightarrow \left(CN(t), CC(t), SV(t)\right)\end{aligned}, \tag{14}$$

Мұндағы, $UM = \left(UM_i\right)$ – БҰ-ны жалпыланған $pa_i^{Ba}, \forall i$ түрлендіру ережелерінің векторы pa_i^B.

(14) өрнек ШҚТ-ға белгілер жиынтығымен сипатталатын КҚ АҚ ұғымдарын түсіндіруге және жалпылауға мүмкіндік береді.

Осылайша, (15) өрнекті қолдана отырып, БӨ көрсету (репрезентация) моделі келесі кортежбен анықталады:

$$\left\langle SC_{pa}, FS_{si}, UM\right\rangle, \tag{15}$$

мұндағы, SC_{pa} – БӨ ҰЖ, FS_{si} – БӨ ФЖ

сонымен қатар, $\left\langle U(PA), WH, PA^i, \left(CN(t), CC(t), SV(t)\right)\right\rangle$.

Қорытынды табу және шешім қабылдау міндеті жағдайды АҚ-ның ағымдағы жағдайынан мақсатты жағдайға өзгерту стратегиясын әзірлеуге дейін азаяды. Осылайша, кері есеп шешіледі.

Шешім қабылдау барысында БӨ үшін анықталады:

$$X(0) = \left(x_{11}^{0},..., x_{nm}^{0}\right) \tag{16}$$

және

$$X^{P} = \left(x_{11}^{p},..., x_{nm}^{p}\right). \tag{17}$$

Кейбір жағдайларда шешім болмаған кезде прецеденттер болуы мүмкін. Алайда, жағдайдың когнитивтік моделінің құрылымын өзгертуде эвристикалық тәсілді қолдану арқылы, соның ішінде АҚ сарапшыларын тарту арқылы шешім табуға болады. Шешімдерді іздеу келесі кезеңдерді қамтиды:

- қорытындыларды генерациялау;
- функционалды көрсету үшін қорытындыларды құрылымдау;
- ұғымдық форматтағы қорытындыларды құрылымдау.

Ғылыми жұмыста АО КҚ қамтамасыз ету міндеттерінде қолданылатын ШҚҚЖ тұжырымдамасы қарастырылды. Аталған ШҚҚЖ әлсіз құрылымдалған деректер жағдайында анықталған ауытқулар белгілері мен кибершабуылдар салдарын бағалау міндеттерінде қолданылады. Сондай-ақ, аномалиялар мен шабуылдардың жекелеген түсіндіруге қиын белгілерін анықтауға арналған ШҚҚЖ ББ қалыптастыру және қолдану процесінің тұжырымдамалық және функционалдық аспектісінде сипаттама моделі көрсетілген. Ғылыми зерттеудің болашағы – киберқауіпсіздікте шешімдерді қабылдауды қолдау жүйесіндегі метабілімді сипаттау моделін дамыту.

Қорытынды

Ғылыми жұмыста төмендегідей нәтижелер алынды:

АО КҚ қамтамасыз ету міндеттерінде қолданылатын ШҚҚЖ тұжырымдамасы ұсынылды. Атап айтқанда, ШҚҚЖ жекелеген модульдері әлсіз құрылымдалған белгілер мен анықталған ауытқулар деректері жағдайында кибершабуылдардың салдарын бағалау үшін деректерді талдау міндеттерінде пайдаланылады. Жоғарыда ұсынылған модельдерге сүйене отырып, киберқауіпсіздік шешімдерін қолдау жүйесіндегі метабілімдерді сипаттауға арналған модульдер құрылымы жасалды.

АО киберқорғау процестерін түсінуді арттыруға мүмкіндік беретін аномалиялар мен шабуылдардың жеке түсіндіруге қиын белгілерін анықтауға байланысты жағдайлар үшін ШҚҚЖ ББ қалыптастыру және қолдану процесінің тұжырымдамалық және функционалдық аспектісінде сипаттама моделі жасалды. Әзірленген үлгі мен модельдер әртүрлі кезеңдерде әлсіз құрылымдық белгілермен сипатталуы мүмкін басып кіруді анықтау кезінде ШҚҚЖ есептеу ядросын құрайды. ШҚҚЖ ББ қалыптастыру және қолдану процесінің тұжырымдамалық және функционалды жағына арналған сипаттама моделі аномалиялар мен шабуылдарды жеке түсіндіру, аномалиялар мен шабуылдар белгілерін анықтау қиын жағдайларда пайдалануға мүмкіндік береді.

Пайдаланылған әдебиеттер тізімі:

1 Палаева, Л. В., Хафизов, А. М., Гилязетдинова, А. М., Вахитова, А. Р., Давыдова, К. Н., & Сиротина, Е. Р. (2017). Основные виды кибератак на автоматизированные системы управления технологическим процессом и средства защиты от них. Фундаментальные исследования, (10-3), 507-511.

2 Пижевский, Д. Е., Антонов, В. О., Заволокина, У. В., Унтевский, Н. Ю., & Тебуева, Ф. Б. (2019). Анализ мировой тенденции роста киберугроз на основе линейной аппроксимации статистических данных об атаках. In Студенческая наука для развития информационного общества (pp. 118-127).

3 Купрюшин, С. А. (2019). Кибер-угрозы и их влияние на мировую экономику и экономику россии. проблемы российских компаний по борьбе с кибер-угрозами. In Инновационные доминанты социально-трудовой сферы: экономика и управление (pp. 159-163).

4 Отчет за 2020 г. с результатами глобального опроса директоров по информационной безопасности - https://www.cisco.com/c/ru_ru/products/security/security-reports.html

5 Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, А. В. Котенко // Тр. СПИИРАН. 2016. № 2 (45). С. 207-244.

6 Petit, J. Potential Cyberattacks on Automated Vehicles [Text] / J. Petit, S. E. Shladover // IEEE Transactions on Intelligent Transportation Systems. – 2015. – Vol. 16, Iss. 2. – P. 546 – 556. DOI: 10.1109/TITS.2014.2342271

7 Кулинич А.А. Концептуальные «каркасы» плохо определенных предметных областей. Открытые семантические технологии проектирования интеллектуальных систем: материалы III Международной научно-технической конференции (Минск, 21–23 февраля 2013 г.) / под ред. Голенкова В.В. – Минск: БГУИР, 2013, с. 135–142.

8 Akhmetov, B., Lakhno, V., Boiko, Y., & Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Восточно-Европейский журнал передовых технологий, (1 (2)), 4-15.

9 Li-Yun Chang, Zne-Jung Lee (2013). Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system, International Conference on Fuzzy Theory and Its Applications (iFUZZY), P. 346 – 351.

10 Кулинич А.А. Концептуальные «каркасы» плохо определенных предметных областей. Открытые семантические технологии проектирования интеллектуальных систем: материалы III Международной научно-технической конференции (Минск, 21–23 февраля 2013 г.) / под ред. Голенкова В.В. – Минск: БГУИР, 2013, с. 135–142.

11 Мусихина, Д. А., Яньков, П. А., & Елизарова, А. А. (2017). Выявление комплексных кибератак на критически важных объектах. Успехи современной науки, 4(2), 60-64.

12 Корченко, А. А., & Жумангалиева, Н. К. (2018). Структурная модель системы выявления вторжений. In Новые информационные технологии и системы (pp. 171-173).

13 Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. ICT Express, 4(2), 95-99.

14 Kabir, E., Hu, J., Wang, H., & Zhuo, G. (2018). A novel statistical technique for intrusion detection systems. Future Generation Computer Systems, 79, 303-318.

References:

1 Palaeva, L. V., Hafizov, A. M., Gilyazetdinova, A. M., Vahitova, A. R., Davydova, K. N., & Sirotina, E. R. (2017). Osnovnye vidy kiberatak na avtomatizirovannye sistemy upravleniya tekhnologicheskim processom i sredstva zashchity ot nih [The main types of cyber attacks on automated process control systems and means of protection against them]. Fundamental'nye issledovaniya, (10-3), 507-511. (In Russian)

2 Pizhevskij, D. E., Antonov, V. O., Zavolokina, U. V., Untevskij, N. YU., & Tebueva, F. B. (2019). Analiz mirovoj tendencii rosta kiberugroz na osnove linejnoj approksimacii statisticheskih dannyh ob atakah [Analysis of the global trend in the growth of cyber threats based on a linear approximation of statistical data on attacks]. In Studencheskaya nauka dlya razvitiya informacionnogo obshchestva. 118-127. (In Russian)

3 Kupryushin, S. A. (2019). Kiber-ugrozy i ih vliyanie na mirovuyu ekonomiku i ekonomiku rossii. problemy rossijskih kompanij po bor'be s kiber-ugrozami [Cyber threats and their impact on the world economy and the Russian economy. problems of Russian companies in combating cyber threats]. In Innovacionnye dominanty social'no-trudovoj sfery: ekonomika i upravlenie. 159-163. (In Russian)

4 Otchet za 2020 g. s rezul'tatami global'nogo oprosa direktorov po informacionnoj bezopasnosti - https://www.cisco.com/c/ru_ru/products/security/security-reports.html (In Russian)

5 A.A. Branickij, A.V. Kotenko (2016) Analiz i klassifikaciya metodov obnaruzheniya setevyh atak [Analysis and classification of network attack detection methods]. A.A. Branickij, A.V. Kotenko. Tr. SPIIRAN. 2016. № 2 (45). 207-244. (In Russian)

6 Petit, J. Potential Cyberattacks on Automated Vehicles [Text] / J. Petit, S. E. Shladover // IEEE Transactions on Intelligent Transportation Systems. – 2015. – Vol. 16, Iss. 2. – P. 546 – 556. DOI: 10.1109/TITS.2014.2342271

7 Kulinich A.A. (2013) Konceptual'nye «karkasy» ploho opredelennyh predmetnyh oblastej. Otkrytye semanticheskie tekhnologii proektirovaniya intellektual'nyh system [Conceptual "frameworks" of poorly defined subject areas. Open semantic technologies for designing intelligent systems]: materialy III Mezhdunarodnoj nauchno-tekhnicheskoj konferencii. pod red. Golenkova V.V. Minsk: BGUIR, 135–142. (In Russian)

15 Akhmetov, B., Lakhno, V., Boiko, Y., & Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Восточно-Европейский журнал передовых технологий, (1 (2)), 4-15.

16 Li-Yun Chang, Zne-Jung Lee (2013). Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system, International Conference on Fuzzy Theory and Its Applications (iFUZZY), p. 346 – 351.

8 Kulinich A.A. (2013) Konceptual'nye «karkasy» ploho opredelennyh predmetnyh oblastej [Conceptual "frameworks" of ill-defined subject areas]. Otkrytye semanticheskie tekhnologii proektirovaniya intellektual'nyh sistem: materialy III Mezhdunarodnoj nauchno-tekhnicheskoj konferencii (Minsk, 21–23 fevralya 2013 g.) / pod red. Golenkova V.V. Minsk: BGUIR, 135–142. (In Russian)

9 Musihina, D. A., YAn'kov, P. A., & Elizarova, A. A. (2017). Vyyavlenie kompleksnyh kiberatak na kriticheski vazhnyh ob"ektah [Detection of complex cyber attacks on critical facilities]. Uspekhi sovremennoj nauki, 4(2), 60-64. (In Russian)

10 Korchenko, A. A., & ZHumangalieva, N. K. (2018). Strukturnaya model' sistemy vyyavleniya vtorzhenij [Structural model of an intrusion detection system]. In Novye informacionnye tekhnologii i sistemy. 171-173. (In Russian)

11 Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. ICT Express, 4(2), 95-99.

12 Kabir, E., Hu, J., Wang, H., & Zhuo, G. (2018). A novel statistical technique for intrusion detection systems. Future Generation Computer Systems, 79, 303-318.