ӘОЖ 004.33(035)
https://doi.org/10.47533/2023.1606-146X.10

Б. Е. ЯГАЛИЕВА[1]*, В. А. ЛАХНО[2] , К. К. МАКУЛОВ[1]

[1]Есенов университеті, Ақтау қ., Қазақстан
[2]Украина биоресурстар және табиғатты пайдалану ұлттық университеті, Киев қ., Украина

ҚОРҒАНЫС ЖАҒЫНДАҒЫ ҚАТЕРЛЕР МЕН РЕСУРСТАРДЫҢ БҰЛДЫР ЖИЫНТЫҒЫМЕН КИБЕРҚАУІПСІЗДІКТІ ҚАРЖЫЛАНДЫРУДЫҢ АДАПТИВТІ МОДЕЛІ

Мақалада шабуылдаушы тараптың қаржылық ресурстары туралы толық ақпараты жоқ ақпараттандыру объектісінің киберқауіпсіздік құралдарын қаржыландыру стратегияларын таңдаудың адаптивті моделі ұсынылған. Жағдай қорғаныс тарапының қаржылық ресурстары бұлдыр жиынтыққа жатқанда қаралады. Модель ақпараттық қауіпсіздік жүйелеріне инвестициялаудың ұтымды нұсқаларын таңдау міндеттерінде шешімдерді қолдау жүйесіне арналған. Шешім бірнеше терминалды беткейлері бар көпқадамды ойындар теориясының құралдарын қолдану негізінде алынды. Шешімдерді іздеу үшін бірнеше терминал беткейлері бар бейтарап жүрістермен сызықты емес көпқадамды ойын аппараты қолданылды. Ақпараттандыру объектісінің қауіпсіздігі кездейсоқ сипаттағы киберқауіптерді жүзеге асырумен байланысты зиян негізінде анықталады. Ақпараттық объектілер қауіпсіздік индикаторы қауіптер жиынтығының қауіптілік коэффициенті мен ақпараттық объекті қауіпсіздік дәрежесі арасындағы анық емес қатынастар матрицасы арқылы анықталады. Модель қорғаныс жағында шабуылдаушы тараптың қаржылық стратегиялары туралы да, оның ақпаратты қорғаудың шараларын еңсеруге бағытталған оның қаржылық ресурстарының жағдайы туралы да толық ақпарат жоқ деген болжаммен ерекшеленеді. Қорғаныс жағы өзінің қаржылық ресурстарының бір бөлігі есебінен қосымша ақпарат алуға мүмкіндігі бар деп болжануда. Модельдің өнімділігі есептеу экспериментінің көмегімен тексерілді, және оның нәтижелері мақалада көрсетілген.

Түйін сөздер*: ақпаратты қорғау, ақпараттандыру объектісі, ойын теориясы, қаржылық стратегия, түсініксіз жиынтықтар, қосымша ақпарат алу тәртібі, шешімдерді қолдау жүйесі.*

Кіріспе. Бүгінгі таңда кез-келген ақпараттандыру объекті (АО) өзінің ақпараттық ресурстарын қорғауды қажет етеді. Қазірдің өзінде барлық ақпараттық объектілер (АО) мен олардың ақпараттық жүйелерін (АЖ) жобалау кезеңінде бюджетке тиісті ақпараттық қорғау жүйелерін (АҚЖ) және КрҚ құру немесе жаңарту үшін қаражат бөлінеді. Сонымен қатар, біз ақпараттандыру объекті неғұрлым күрделі болғанын атап өтеміз, мысалы, университеттік ақпараттық жүйесін [1] банкті [2] қорғауды салыстырсақ, сәйкесінше киберқауіпсіздік контуры қорғау жағында болуы керек [3, 4].

Қазіргі заманғы АҚЖ және КрҚ – бұл антивирустық бағдарламалық жасақтаманы, файрволдар, желідегі шабуылдар мен ауытқуларды анықтауға арналған жүйелерді, криптографиялық қосымшаларды және т.б. қамтитын кешендер [1, 3, 4].

Ақпараттық объектілерге немесе аса маңызды сыни компьютерлік жүйелерге кибер шабуылдардың сценарийлері күрделене түскендіктен, киберқауіпсіздік құралдары мен жүйелерін таңдау үшін қорғаныс жағында дәстүрлі стратегияларға негізделген ақпараттық қауіпсіздік жүйелерінің кешендері мен контурларының аппараттық-

* E-mail корреспондирующего автора: bagdat.yagaliyeva@yu.edu.kz

бағдарламалық құрамын алдын-ала қалыптастыру қиынға соғып жатқанын ескереміз. Қорғаныс жағы киберқауіптердің ландшафтының өзгеруін динамикалық түрде ескеруі қажет болатын нақты жағдай болып шығуы мүмкін, бұл ақпараттық объектінің қорғаныс контурларын қайта қарау немесе қайта конфигурациялау қажеттілігіне әкеледі. Бұл, өз кезегінде, жаңа файрволды, кіруді анықтау жүйелерін және сол сияқтыларды сатып алуға қосымша қаржылық шығындармен байланысты. Бұлдыр қауіпті қауіптер мен жаңа қауіптер мен шабуыл сценарийлерінің пайда болу тенденциясын ескере отырып, киберқылмыскерлерге қарсы стратегияның қаржылық құрамын таңдау мәселесін шешу динамикалық міндет деп айта аламыз. Сонымен бірге нақты жағдайларда қорғаныс жағының көптеген ресурстары бұлдырлықтың белгілі бір параметрлеріне сәйкес келеді деп айтуға болады.

Өздеріңіз білетіндей, көп жағдайда нақты физикалық әлемде кездесетін объектілер кластарында мүшелік критерийі дәл анықталмаған. Сонымен бірге, дәл осындай анықталмаған «сыныптар» адамның ойлауында, атап айтқанда, информатика, кибернетика, жасанды интеллект, заңдылықты тану, ақпарат беру және абстракциялау және басқа да салаларда маңызды рөл атқаратындығы даусыз факт.

Буылдыр жиынның тұжырымдамасы көптеген жиынтықта қарапайым жиынтықтарда қолданылатындарға параллель болатын, бірақ соңғыларына қарағанда жалпы, ал кеңірек болуы мүмкін тұжырымдамалық негіздерді құруға ыңғайлы бастама болатындығын ескеру қажет. Атап айтқанда, бұл келесі салаларға қатысты: суреттерді жіктеу; мәліметтерді өңдеу; ойын теориясы және т.б.

Маңыздысы, мұндай құрылымдар кездейсоқ шамалардың болуына емес, сыныпқа кірудің нақты анықталған критерийлерінің болмауына байланысты болатын дәлсіздік көзі есептерді шешудің табиғи әдісін ұсынады. Сондықтан, осы мақалада қарамақайшылықты сипаттағы мәселелерді шешуге тырысады және онда ақпараттың толық еместігі стохастикалық сипатта болмайды, бірақ бұлыңғыр жиындар берген анық емес ақпарат сипатына ие болады.

[4-6]-де кешенді КрҚ пен АҚЖ құрудағы негізгі мәселелердің бірі АО үшін КрҚ пен АҚЖ инвестициялаудың ұтымды стратегиясын таңдау екендігі көрсетілген. Ақпараттандыру объектісі үшін киберқауіпсіздік міндеттері саласындағы [6, 7] шешімдерді қабылдауды қолдау интеллектуализациясының соңғы жылдары қалыптасқан тенденциясы осындай жүйелер үшін әлі шешілмеген мәселелерге жаңаша көзқараспен қарауға мүмкіндік берді. Атап айтқанда, АҚЖ және КрҚ қаржыландырудың ұтымды стратегияларын таңдаудың жаңа модельдерін әзірлеу міндеті өзекті болып қала береді. Мысалы, бұл қорғаныс жағы жаңа бұзу технологияларымен бетпе-бет келуі мүмкін жағдайларда қажет. Бұл өз кезегінде ақпараттандыру объектісі үшін киберлік тәуекел деңгейлерін өзгертеді. Сондықтан, сайып келгенде, қорғаныс тарабы ұтымды стратегияны таңдау үшін КрҚ пен АҚЖ қаржыландыру стратегияларын қайта қарау қажет болғанда жағдай туындауы мүмкін.

Мақаланың мақсаты – ақпараттандыру объектісінің киберқорғанысын қаржыландырудың ұтымды стратегияларын таңдау бойынша шешімдерді қолдау жүйелерінің моделін жасау.

Мақаланың негізгі материалы. Ақпараттандыру объектісінің қауіпсіздігі кездейсоқ сипаттағы киберқауіптерді жүзеге асырумен байланысты зиян негізінде

анықталады. Бұл жағдайда қауіптілік коэффициенттері ақпараттық қауіпсіздік жүйесінің нақты параметрлерімен корреляцияланады. Бұл параметрлердің бірі - ақпараттық қауіпсіздік жүйесінің баға-сапа қатынасы. Сонымен параметрлер немесе олардың жиынтығы анық емес мәндермен ұсынылады, ал АО қауіпсіздік индикаторы қауіптер жиынтығының қауіптілік коэффициенті мен АО қауіпсіздік дәрежесі арасындағы анық емес қатынастар матрицасы арқылы анықталады.

Ақпараттандыру объектісінде ақпаратты техникалық қорғау құралдарының (АТҚҚ) тиімділігін бағалауға көзқарас АТҚҚ қолданбай қауіпсіздік көрсеткіштерін салыстырмалы талдауға негізделген. Сонымен, біз ақпараттандыру объектісіне антропогендік және техногендік қауіптің қауіптілік дәрежесін анық емес ұсыну шарттары туралы айтып отырмыз. Талдау объектілерінің, қауіп-қатерлердің құрамы мен сипаттамаларының күрделілігінің жоғарылауына байланысты (бірінші кезекте, біз қашықтан рұқсат етілмеген қатерлер туралы айтамыз), ақпараттандыру объектісі мен аса маңызды компьютерлік жүйелердің (АМКЖ) қауіпсіздігін сандық бағалау міндеті өзекті болып табылады. АТҚҚ тиімділігін бағалау келесі тәсілдер негізінде мүмкін: 1) қауіпсіздік көрсеткішінің мәнін нормативпен (шекті) салыстыру; 2) АТҚҚ [7-15] және ақпаратты техникалық қорғау құралдарынсыз салыстыру.

Екі тәсіл де белгілі бір модельдер мен әдістер деңгейінде қолданылады. Тиімділікті кешенді бағалау үшін бірінші тәсіл өте қолайлы емес, өйткені қазіргі заманғы киберқауіптер кешенінен ақпараттандыру объектісі мен АМКЖ қауіпсіздігін төмендетудің қолайлы деңгейлерін анықтау қиын. Екінші тәсіл АТҚҚ шаралары мен құралдарының тиімділігін салыстырмалы талдауда қолданылады және АТҚҚ жеткіліктілігін анықтауға мүмкіндік бермейді.

АО күрделене түсуімен, АҚ пен КрҚ төнетін қатерлер жиынтығы мен сипатының өзгеруімен, әсіресе АМКЖ ресурстар мен процестерге қашықтықтан рұқсатсыз қол жетімділік қатерлерімен, қауіпсіздікті сандық бағалау міндеті өзекті болып табылады. АО мен АМКЖ үшін АМКЖ қауіпсіздігін және киберқорғаныс стратегиясының қаржылық компонентін әзірлеуді дұрыс бағалау мақсатқа және күрделілік деңгейіне ұқсас жүйелерді салыстыру немесе бақылау үшін қажет уақыт бойынша белгілі бір ақпараттандыру объектісінің қауіпсіздік деңгейінің динамикасы.

Практикалық есептерді шешу кезінде қарастырылатын есептің моделін нақтыға дәйекті жақындату процедурасы қолданылады. Тиісінше, қарапайым модель шеңберінде мәселені шешу негізінде нақты проблеманың шешімін табуға болады – АО қорғаныс жүйелерін қаржыландырудың ұтымды стратегиясын анықтау.

Мысалы, [13]-де бірінші ойыншының таңдаулы жиынтықтары табылған және оның оңтайлы стратегиялары табылған жағдайлар қарастырылды. Бұл дегеніміз, егер ойыншылардың күйлері бірінші ойыншының артықшылықтарының жиынтығына жататын болса, онда оның стратегиясы бар, оны жүзеге асыру мақсатына жетуге мүмкіндік береді. Осылайша, берілген ықтималдықпен 1 ойыншы (яғни, ақпаратты қорғаушы - АҚ) жүйені өзі үшін оң нәтиже көрсететін күйге келтіреді. Алайда, жағдай қорғаушыдан ойын ережелерінің стандартты белгілеуін жасай алмайтын мемлекеттерден оған оң нәтиже алу қажет болған жағдайда мүмкін болады. Мысалы, ол өзара әрекеттесу уақытында шектеулі. Содан кейін оларды алудың өзіндік ресурстарының бір бөлігі есебінен қосымша ақпарат алу процедурасын енгізу орынды сияқты.

Бұл процедура, егер ақпараттың толық еместігі стохастикалық немесе анық емес сипаттағы сипатқа ие болса, өте маңызды. Сонымен бірге бұлыңғыр ақпарат шынайы өмірге тән екенін ескеру қажет. Сонымен, сарапшылардың бағалауы жағдайында сарапшылардың тұжырымдарының екіұштылығы сөзсіз, бұл үшін мұндай проблемаларды шешу құралдарын әзірлеу қажет, әсіресе жанжалды жағдайға байланысты белгісіздік қосылса. Тәжірибе көрсеткендей, мұндай жағдайларда тиімді құралдардың бірі ойын теориясын қолдану болып табылады.

Міндеттің қойылуы. Ақпараттық қорғаушыны қаржыландыру проблемасы оның ішкі тапсырманы және қосымша ақпарат алудың тиісті тәртібін енгізе отырып, хакерлік тарапқа қарсы әрекеті шеңберінде қарастырылады. Қосымша ақпаратты АҚ алу үшін ресурстарының бір бөлігін жұмсау есебінен ала алады. Осыған ұқсас зерттеулерден айырмашылығы, жағдай қорғаныстың қаржылық ресурстарына қатысты түсініксіз ақпарат болған кезде қарастырылады.

Есептің шешімі. Белгілі бір уақыт аралығында $\{0,1,...,T\}$ (T – натурал сан), ақпараттық қауіпсіздікке $x(0)$ қаржылық ресурстар бөлінген деп есептейміз. Екінші ойыншы, сәйкесінше – $y^{\xi}(0)$.

Бұл ресурстар $t = 0$ уақытында болжанған, ойыншылардың өз мақсаттарына жетуі керек қаржылық ресурстарының көлемін анықтайды. Ойыншылар арасында өзара байланыс бар. Бұл өзара әрекеттесу анық емес ақпаратпен кезектесіп жүретін екі сатылы ойын ретінде сипатталатын болады. Ақпаратты қорғау туралы толық ақпараты бар ойыннан айырмашылығы, екінші ойыншының бастапқы күйі нақты белгісіз.

Алайда, ақпараттық қауіпсіздік екінші ойнатқыштың күйлері анық емес жиынтыққа жататындығы белгілі $\{X, m(.)\}$. Мұндағы анық емес жиынтықтың тасымалдаушысы $[ar, b + r]$ кесіндісі, a, b, r – оң сандар, $b \geq a$, $a \geq r$, $b - a \geq 2 \times r$; және m (.) мүшелік функциясы келесідей анықталады:

$$\mathrm{m(x)} = \left\{0,\ x \leq a - r, \left(\frac{1}{2\times r}\right) \times (x - a + r), a - r \leq x \leq a + r, 1, a + r \leq x \leq b - r, \left(-\frac{1}{2\times r}\right) \times (x - b - r), 0, x \geq b + r; \right\}; \quad (1)$$

Сондай-ақ, бірінші ойыншы біледі:

1) тараптардың өзара іс-қимылын анықтайтын бастапқы күй және параметрлер;

2) $x(\tau)$ для $\tau \leq$ t. үшін оның барлық күйлері $x(\tau)$.

Бірінші ойыншы (АҚ) өзінің қаржылық ресурстарының бір бөлігі есебінен қосымша ақпарат ала алады деп саналады. Бұл бірінші ойыншының ресурсының бөлігін анықтайтын $k(k \in [0,1])$ параметрін енгізу нәтижесінде пайда болады. Қаржы ресурстарының бұл бөлігі $(1-k) \cdot$ z тең. Z – бұл ақпарат алу үшін қолданылатын ресурстың мәні (АҚ) деп ойлаймыз. Ақпарат алу үшін пайдаланылатын z – ресурстардың мәні (АҚ) деп ойлаймыз.

Бұл қосымша ақпарат екінші ойыншының (хакердің) y^{ξ} күйіне қатысты және $\{Y, m(.)\}$, айқын емес жиынтыққа жатады, мұндағы $Y = [a - k^2\mathrm{r}, b + k^2r]$, a, b, r – оң сандар, $b \geq a$, $a \geq r$, $b - a \geq 2 \times r$. $m(.)$ – тиесілі функциясы келесідей анықталған:

$$\mathrm{m(x)} = \left\{0,\ x \leq a - k^2r, \left(\frac{1}{2\times k^2r}\right) \times (x - a + k^2r), a - k^2r \leq x \leq a + k^2r, 1, a + k^2r \leq x \leq b - k^2r, \left(-\frac{1}{2\times k^2r}\right) \times (x - b - k^2r), 0, x \geq b + k^2r; \right\}. \quad (2)$$

Дәлелдеу бірінші ойыншының позициясынан жүзеге асырылады (яғни АҚ). Сондықтан екінші ойыншының (хакердің) сана-сезімі туралы ешқандай болжамдар жасалмайды. Ойыншылардың қадамдары кезек-кезек орын алады. Жұп моментте бірінші ойыншы қадам жасайды, тақ моментте екінші.

$t = 2n$ және $x(t)$, $x(t + 1)$ бірінші ойыншының t, $t + 1$ уақытының моменттеріндегі күйлері болсын. Сондай-ақ t, $t + 1$ уақыттағы моментте екінші ойыншының күйлері. Содан кейін ойыншылардың $t + 1$, $t + 2$ уақытындағы күйлері қатынастардан анықталады:

$$x(t+1) = k(t)\cdot\alpha\cdot x(t) - u(t)\cdot k(t)\cdot\alpha\cdot x(t);\ y^{\xi}(t+1) = y^{\xi}(t) - s_1\cdot u(t)\cdot k(t)\cdot\alpha\cdot x(t); \quad (3)$$

$$y^{\xi}(t+2) = \beta\cdot y^{\xi}(t+1) - v(t)\cdot\beta\cdot y^{\xi}(t+1);\ x(t+2) = x(t+1) - s_2\cdot v(t)\cdot\beta\cdot y^{\xi}(t+1); \quad (4)$$

Мұнда $u(t), v(t), k(t) : u(t) \in [0,1],\ v(t) \in [0,1], k(t) \in [0,1];\ s_1 > 0,\ s_2 > 0.$

$y \le x\}$ үшін $F(.): R \to R, F(x) = \{sup\ sup\ m(y)$ функциясын анықтайық (5)

$\{X_t, m_t(.)\}, (t = o, 1, \ldots)$ – екінші ойыншының күйлері осылай анықталған ойыншылар күйінің динамикасына жататын бұлыңғыр жиынтықтармен белгілейік; $y \le x\}$ арқылы: $F_t(.): R \to R, F_t(x) = \{sup\ sup\ m_t(y)$.

Ойынның толық сипаттамасын біз [12, 13] жұмысында келтірдік.

Сондықтан, осы мақала аясында біз шабуылдаушы (хакер) қимыл жасағаннан кейін $x(t + 2) > 0$ шарты $< p_1$, $(0 \le p_1 \le 1)$ сенімділігімен қанағаттанатын жағдайды қарастыруға назар аударды қ. Яғни, шабуылдаушы $(1 - p_1)$ тен жоғары сенімділікке ие ақпараттық жүйелерді бүлдірді деп айтуға болады.

Яғни, шабуылдаушы сенімділігі $(1 - p_1)$-ден жоғары ақпараттық жүйелерді бүлдірді деп айта аламыз. Содан кейін осы қорғаныс кедергілерін конфигурациялау үшін киберқауіпсіздікті қаржыландыру процедурасы аяқталды. Содан кейін осы қорғаныс кедергілерін конфигурациялау үшін киберқауіпсіздікті қаржыландыру процедурасы аяқталды.

Әйтпесе, процедура жалғасуда.

[12, 15]-дегідей, бірінші ойыншы келесі қасиетке ие бастапқы күйлерінің жиынын (КЖ) табуға ұмтылады. Қасиет: егер ойын бастапқы күйлерден басталса, онда бірінші ойыншы өзінің басқару әрекеттерін $u(0)$, $k(0)$,..., $u(t)$, $k(t)(t = 2n)$ таңдай отырып, өзінің ақпараттық жүйелерінің сенімділігін p_0-дан жоғары қорғауды қамтамасыз ете алады.

Сонымен бірге, ақпараттық қорғаушы хакердің зиян келтіруіне үлкен сенімділікпен тосқауыл қоя алады. Мұндай күйлер жиынтығы бірінші ойыншының қалау жиыны деп аталады.

Сонымен бірге, ақпараттық қорғаушының стратегиясы оған қолда бар ақпарат негізінде киберқауіпсіздік жүйесін дамытуға бағытталған қаржылық ресурстардың көлемін анықтауға мүмкіндік беретін ереже болып табылады. Сондай-ақ, қаражаттың бір бөлігі екінші ойыншы (хакер) туралы қосымша ақпарат алуға бағытталған. Екінші ойыншы кез-келген ақпарат негізінде өзінің $v(.)$ стратегиясын таңдайды.

Бірінші ойыншының мақсаты - оның қалауын табу.

Сондай-ақ, ақпаратты қорғаушыға стратегиялар анықталды, оның көмегімен ол кибер қорғанысты қаржыландыру процедурасын аяқтауға мүмкіндік беретін шарттардың орындалуын алады. Көрсетілген қасиеттері бар бірінші ойыншының стратегиялары оның оңтайлы стратегиялары деп аталады.

Ойынның тұжырымдалған моделі, шешім қабылдау теориясының жіктелуіне сәйкес, түсініксіз ақпарат жағдайында шешім қабылдау проблемасына сәйкес келеді. Мұндай модель – кезек-кезек жүретін бірнеше терминал беткейлері бар сапасыз көпсатылы ойын екенін ескеріңіз.

Бірінші ойыншыға (АҚ) арналған артықшылық жиынын және оның оңтайлы стратегияларын табу параметрлер жиынтығына байланысты екенін ескеру қажет.

Қорғаныс тарапында буылдыр жиынтықпен сипатталатын ресурстар болған кезде және ол бірінші қадамда ақпарат алу процедурасын қолданған кезде ойыншының жағдайды таңдаған жұмысын [13,15] ескере отырып, келесі өрнектер алынды.

$p_1 = p_0$ жағдайын береміз.

T қадамындағы бірінші ойыншының бірінші қадамдағы қосымша ақпараттық процедураны қолданатын іс үшін артықшылықтарының жиынтығы $V_{1,k(1)}^{T}(p_0, p_0)$ - мен белгіленеді.

[13,15]-де ойыншылардың оңтайлы стратегияларының оңтайлылық жиындарының белгісі келтірілген, осы мақалада жиындардың және қарапайым жағдайға арналған оңтайлы стратегиялардың белгілерін ұсынамыз.

$T = 1$

$p_0 : 0 \le p_0 \le 0{,}5$ кезінде $V_{1,k(1)}^{T}(p_0, p_0)$ аламыз.

$p_0 : 0{,}5 < p_0 < 1$ кезінде, аламыз:

Егер $a < 2 \cdot p_0 \cdot r - r$, онда

$$V_{1,k(1)}^{1}(p_0, p_0) = \left\{x(0) : 2\sqrt{a(2 \cdot p_0 \cdot r - r)} \le s_1 \cdot \alpha \cdot x(0) < a + 2 \cdot p_0 \cdot r - r\right\},$$

Ақпаратты қорғаушы үшін оңтайлы стратегия $[u(.,.,.), k(.,.,.)]$ функциясының жұбы болады:

$$\left(\bar{k}(1)\right)_2 < k^*(x(0), F(.)) < \left(k(1)\right)_1,$$

$$\left(\bar{k}(1)\right)_{1,2} = \frac{s_1 \cdot \alpha \cdot x(0) \pm \sqrt{(s_1 \cdot \alpha \cdot x(0))^2 - 4 \cdot a(2 \cdot p_0 \cdot r - r)}}{2 \cdot (2 \cdot p_0 \cdot r - r)}; \tag{6}$$

$$u^*(x(0), F(.)) = 1; \text{ кезінде } x(0) : 2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)} \le s_1 \cdot \alpha \cdot x(0). \tag{7}$$

$$u^*(x(0), F(.)) = 0; \text{ кезінде } x(0) : s_1 \cdot \alpha \cdot x(0) < 2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)}. \tag{8}$$

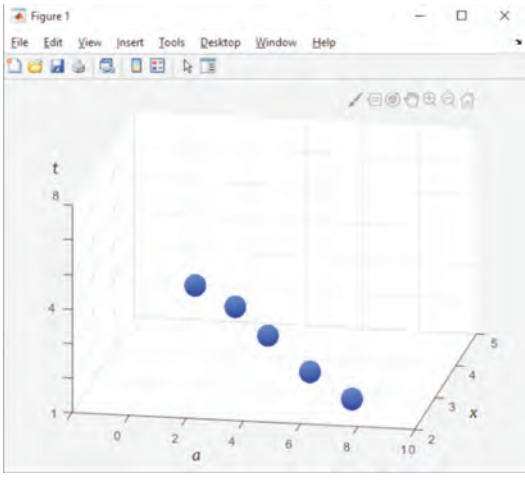
$a \ge 2 \cdot p_0 \cdot r - r$ кезінде $V_{1,k(1)}^{1}(p_0, p_0) = \emptyset$ аламыз.

Айқын емес жиынтықтың ортасын сегмент түрінде анықтау қосымша ақпарат алу процедурасын енгізу кезінде үлкен шектеу емес екенін ескеру қажет. Өзіңізді шектеу жеткілікті, мысалы, сегменттің «сол жағында», бұл ойыншылардың оңтайлылық жиынтығы мен оңтайлы стратегиясын анықтауға әсер етпейді.

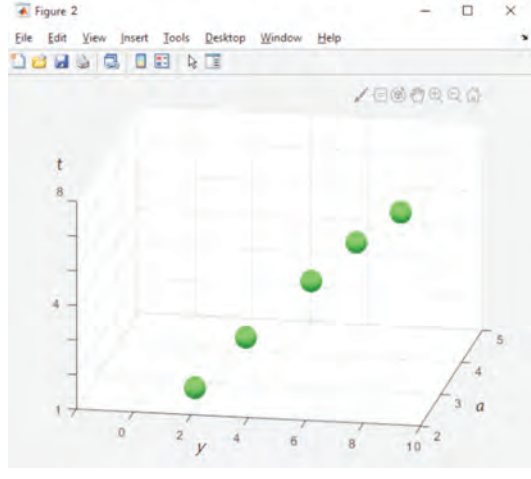
Жұмыста жасалған модельдің тиімділігі мен сәйкестігі жүргізілген тәжірибелермен расталды. Тәжірибелерде ойыншылардың қорғаушы да, шабуылдаушы да стратегияларының жиынтығын анықтауға және сонымен қатар математикалық модельдің сәйкестігін тексеруге міндеттер қойылды.

Төменде 1-3 суреттерде келтірілген үш есептеу экспериментінің нәтижелері келтірілген. 1-3 жағдайлары осы тәжірибелерге сәйкес келеді. Үш жағдай келтірілген. Алайда, шешімдер ойын параметрлерінің барлық жағдайлары үшін алынғанын атап өткен жөн. Жұмыста қарастырылған модельдің көмегімен алынған нәтижелер ақпараттандыру объектісі қорғаушысының өзара әрекеттесу параметрлерінің кез-келген арақатынасы үшін оңтайлы қаржылық стратегияларын табуға мүмкіндік берді.

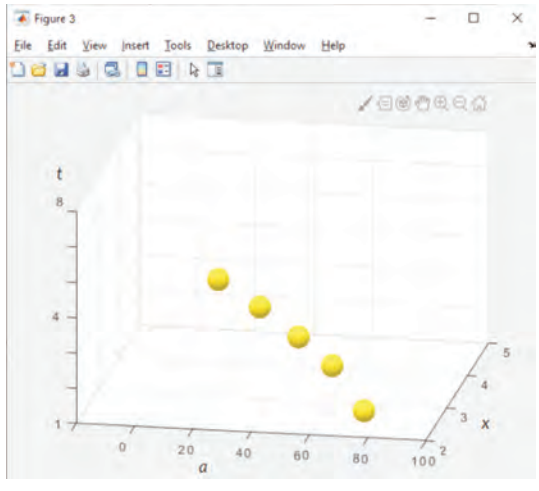
$(t, x(0), a)$ - үш өлшемді кеңістіктегі үш өлшемді оң ортантты қарастырамыз. t уақыт өсі «төменнен жоғарыға, нөлден өтеді». t параметрі ойыншылардың қадамдарының санын білдіреді.



Сурет 1 – Жағдай 1



Сурет 2 – Жағдай 2



Сурет 3 – Жағдай 3

Уақыттың әр сәтінде жүйенің күйі 1-суретте «сары доппен» сипатталған. Ойыншылар оңтайлы стратегияларды қолданғанда жүйенің күйі тепе-теңдік сызығы бойымен «қозғалады».

Алғыс. Зерттеулер мен мақалалар Қазақстан Республикасы Білім және Ғылым министрлігі, Ғылым комитетінің қаржылық қолдауымен AP08855887 «Кибернетикалық қауіпсіздік жүйелеріне инвестициялау процесінде интеллектуалды шешімдерді қабылдауды қолдау жүйесін әзірлеу» жобасы аясында жүргізілді.

Қорытынды. Ақпараттандыру объектілерінің киберқауіпсіздік жүйесін қаржыландыру рәсімдерін сипаттайтын модельдерге толықтырулар ұсынылады. Қолданыстағы шешімдерден айырмашылығы, іс қорғаныс жағында шабуылдаушы тараптың қаржылық стратегиялары туралы да, оның ақпараттандыру объектісін қорғау шекараларын еңсеруге бағытталған оның қаржылық ресурстарының жағдайы туралы да толық ақпарат болмаған жағдайда қарастырылады. Бұл жағдайда қорғаныс тарабы өзінің қаржылық ресурстарының бір бөлігі есебінен қосымша ақпарат алуға мүмкіндігі бар. Қорғаныс тарапының қаржылық ресурстары бұлыңғыр жиынтықтың көмегімен сипатталған жағдайда шешім шығарылады. Шешім динамикалық бағдарламалау әдісіне негізделген. Шешімдерді іздеу үшін бірнеше терминал беткейлері бар бейтарап жүрістермен сызықты емес көпқадамды ойын аппараты қолданылды.

ӘДЕБИЕТ

1 Posey, C., Roberts, T., Lowry, P., Bennett, B., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors.

2 Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Information & management, 51(5), pp. 551-567.

3 Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). Digital crime and digital terrorism. Prentice Hall Press.

4 Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. Journal of Information Security, 7(02), p. 49.

5 Kelly, B. B. (2012). Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform. BUL Rev., 92, p. 1663.

6 Goztepe K. Designing Fuzzy Rule Based Expert System for Cyber Security, International Journal of Information Security Science, 2012, Vol. 1, No 1, pp. 13–19.

7 Fielder A., Panaousis E., Malacaria P. et al. Decision support approaches for cyber security investment, Decision Support Systems, 2016, Vol. 86, pp. 13–23.

8 Lakhno V. A. Development of a support system for managing the cyber security, Radio Electronics, Computer Science, Control, 2017, No. 2, pp. 109–116.

9 Cavusoglu H., Mishra B., Raghunathan S. A model for evaluating IT security investments, Communications of the ACM, 2004, Vol. 47, No. 7, pp. 87–92.

10 Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: a real options perspective. Journal of Accounting and Public Policy, 34(5), pp. 509–519.

11 Fielder, A., Konig, S., Panaousis, E., Schauer, S., &Rass, S. (2017). Uncertainty in Cyber Security Investments. arXiv preprint arXiv:1712.05893.

12 Akhmetov, B., Lakhno, V., Boiko, Y., &Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Eastern-European Journal of Eenterprise Technologies, (1 (2)), pp. 4-15.

13 Lakhno V., Malyukov V., Gerasymchuk N. et al. Development of the decision making support system to control a procedure of financial investment, Eastern-European Journal of Enterprise Technologies, 2017, Vol. 6, N. 3, pp. 24–41.

14 Manshaei M. H., Zhu Q., Alpcan T. et al. Game theory meets network security and privacy, ACM Computing Surveys, 2013, Vol. 45, No. 3, pp. 1–39.

15 Malyukov V.P. Discrete-approximation method for solving a bilinear differential game, Cybernetics and Systems Analysis, 1993, Vol. 29, No. 6, pp. 879 – 888.

REFERENCES

1 Posey, C., Roberts, T., Lowry, P., Bennett, B., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors.

2 Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Information & management, 51(5), pp. 551-567.

3 Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). Digital crime and digital terrorism. Prentice Hall Press.

4 Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. Journal of Information Security, 7(02), p. 49.

5 Kelly, B. B. (2012). Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform. BUL Rev., 92, p. 1663.

6 Goztepe K. Designing Fuzzy Rule Based Expert System for Cyber Security, International Journal of Information Security Science, 2012, Vol. 1, No 1, pp. 13–19.

7 Fielder A., Panaousis E., Malacaria P. et al. Decision support approaches for cyber security investment, Decision Support Systems, 2016, Vol. 86, pp. 13–23.

8 Lakhno V. A. Development of a support system for managing the cyber security, Radio Electronics, Computer Science, Control, 2017, No. 2, pp. 109–116.

9 Cavusoglu H., Mishra B., Raghunathan S. A model for evaluating IT security investments, Communications of the ACM, 2004, Vol. 47, No. 7, pp. 87–92.

10 Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: a real options perspective. Journal of Accounting and Public Policy, 34(5), pp. 509–519.

11 Fielder, A., Konig, S., Panaousis, E., Schauer, S., &Rass, S. (2017). Uncertainty in Cyber Security Investments. arXiv preprint arXiv:1712.05893.

12 Akhmetov, B., Lakhno, V., Boiko, Y., &Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Eastern-European Journal of Eenterprise Technologies, (1 (2)), pp. 4-15.

13 Lakhno V., Malyukov V., Gerasymchuk N. et al. Development of the decision making support system to control a procedure of financial investment, Eastern-European Journal of Enterprise Technologies, 2017, Vol. 6, N. 3, pp. 24–41.

14 Manshaei M. H., Zhu Q., Alpcan T. et al. Game theory meets network security and privacy, ACM Computing Surveys, 2013, Vol. 45, No. 3, pp. 1–39.

15 Malyukov V.P. Discrete-approximation method for solving a bilinear differential game, Cybernetics and Systems Analysis, 1993, Vol. 29, No. 6, pp. 879 – 888.

Б. Е. ЯГАЛИЕВА[1], Б. Б. АХМЕТОВ[1], В. А. ЛАХНО[2]

[1]Университет Есенова, г.Актау, Казахстан
[2]Национальный университет биоресурсов и природопользования, г.Киев, Украина

АДАПТИВНАЯ МОДЕЛЬ ФИНАНСИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ ПРИ НЕЧЕТКИХ МНОЖЕСТВАХ УГРОЗ И РЕСУРСОВ У СТОРОНЫ ЗАЩИТЫ

В статье предлагается адаптивная модель выбора стратегий финансирования средств кибербезопасности объекта информатизации при неполной информации о финансовых ресурсах атакующей стороны. Рассмотрен случай, когда финансовые ресурсы стороны защиты принадлежат некоторому нечеткому множеству. Модель предназначена для разрабатываемой системы поддержки принятия решений в задачах выбора рациональных вариантов инвестирования в системы защиты информации. Решение было получено на основе применения инструментария теории многошаговых игр с несколькими терминальными поверхностями. Для поиска решений применен аппарат нелинейной многошаговой игры качества с несколькими терминальными поверхностями с поочередными ходами. Защищенность ОбИ определяют исходя из ущерба, который связан с реализацией киберугроз, носящих случайный характер. Модель отличает допущение, что сторона защиты не имеет полной информации как о финансовых стратегиях атакующей стороны, так и о состояниях его финансовых ресурсов, направленных на преодоление рубежей защиты информации. Сделано допущение, что сторона защиты имеет возможность получения дополнительной информации за счет затраты части своих финансовых ресурсов. Проверка работоспособности модели была выполнена с помощью вычислительного эксперимента, результаты которого также приведены в статье.

***Ключевые слова**: защита информации, объект информатизации, теория игр, финансовая стратегия, нечеткие множества, процедура получения дополнительной информации, система поддержки принятия решений.*

B. E. YAGALIYEVA[1], B. B. AKHMETOV[1], V. A. LAKHNO[2]

[1]Yessenov University, Aktau, Kazakhstan
[2]National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine
e-mail: bagdat.yagaliyeva@yu.edu.kz

ADAPTIVE MODEL OF CYBER SECURITY FINANCING WITH FUZZY SET OF THREATS AND RESOURCES AT THE SIDE OF PROTECTION

The article proposes an adaptive model for choosing strategies for financing cybersecurity means of an informatization object with incomplete information about the financial resources of the attacking party. The case is considered when the financial resources of the side of the defense belong to some fuzzy set. The model is intended for the developed decision support system in the tasks of choosing rational options for investing in information security systems. The solution was obtained based on the use of the tools of the theory of multistage games with several terminal surfaces. The model is distinguished by the assumption that the protection side does not have complete information about both the financial strategies of the attacking side and the state of its financial resources aimed at overcoming the boundaries of information protection. It is assumed that the defense side has the ability to obtain additional information at the expense of part of its financial resources. The performance of the model was checked using a computational experiment, the results of which are also presented in the article.

***Key words**: information security, object of informatization, game theory, financial strategy, fuzzy sets, procedure for obtaining additional information, decision support system.*