DOI: 10.18372/2410-7840.20.12864
УДК 004.056

МОДЕЛИРОВАНИЕ ПРОЦЕДУРЫ ПРИНЯТИЯ РЕШЕНИЙ ПО ФИНАНСИРОВАНИЮ СРЕДСТВ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ УНИВЕРСИТЕТА

Лазат Кыдыралина, Бахытжан Ахметов, Валерий Лахно

В статье предложена модель для оценки стратегий инвестирования в информационно-образовательную среду университета (ИОСУ). Одним из вариантов решения подобных задач, и, в частности, оценивания рисков, связанных с финансированием систем защиты информации и кибербезопасности ОИСУ, является внедрение интелектуализированных систем поддержки принятия решений. Подобные системы позволяют менеджменту учебных заведений принимать рациональные решения по вложению финансовых средств в развитие инструментария защиты ОИСУ. В статье предложена модель для ИСППР по дискретной процедуре финансирования систем защиты информации и кибербезопасности ИОСУ. Отличием модели от существующих, является допущение ограниченности финансовых ресурсов как стороны защиты ИОСУ, так и атакующих. Модель основана на применении инструментария теории многошаговых игр. В статье описано решение билинейной многошаговой игры качества с зависимыми движениями в рамках стратегий защиты ИОСУ. Описаны результаты имитационного эксперимента в рамках выбора финансовых стратегий киберзащиты ИОСУ. Разрабатываемая интелектуализированная система поддержки принятия решений (ИСППР) позволит конечному пользователю оценивать финансовые стратегии при выпоре направлений инвестирования в системы информационной и кибербезопасности ИОСУ. В отличие от существующих моделей, произведено решение билинейной многошаговой игры качества в классе чистых стратегий, и позволяет производить оценку рисков для игроков, которые, соответственно, представляют стороны защиты и атаки для ИОСУ. В ходе имитационного эксперимента были учтены различные соотношения параметров, описывающих процесс финансирования в средства защиты информации и кибербезопасности ИОСУ. На основании результатов имитационного эксперимента и результатов тестирования ИСППР, сделано заключение о рисках утраты финансовых ресурсов для игроков, соответственно на средства киберзащиты и взлома ИОСУ.

Ключевые слова: *кибербезопасность, информационно-образовательная среда университета, многошаговая игра качества, оптимальные стратегии финансирования.*

Введение. Современные цифровизированные средства многих учебных заведений, в частности, университетов подвержены тем же рискам и киберугрозам, что и традиционные информационно-коммуникационные системы в образовании [1, 2]. Вследствие стремительного развития информационно-образовательных средств и систем в университетах (далее ИОСУ) и возрастающего объема данных в рамках университетского трафика, многие образовательные информационно-коммуникационные системы стали привлекательной мишенью для различного рода киберзлоумышленников. Например, раскрытие персональной пользовательской информации, коммерческой тайны и других данных в ИОСУ, могут потенциально привести к ощутимым финансовым и репутационным потерям. В условиях доступности самых разнообразных средств реализации кибератак (например, Probe, DoS/DDoS и др.) одной из важнейших задач, стоящих перед службами, обеспечивающими бесперебойное функционирование ИОСУ, является задача обеспечения киберзащиты. Это, в свою очередь, вызывает необходимость финансового инвестирования в системы кибербезопасности (СКБ) ИОСУ [3, 4].

Одним из вариантов решения подобных задач, и, в частности, оценивания рисков, связанных с финансированием систем кибербезопасности (СКБ) ОИСУ, является внедрение интелектуализированных систем поддержки принятия решений (ИСППР) [4]. Подобные системы позволяют принимать рациональные решения по вложению финансовых средств (ресурсов, далее ФиР) на развитие инструментария защиты ОИСУ [5, 6]. В статье предложена модель для ИСППР по дискретной процедуре финансирования СКБИОСУ [7, 8].

Постановка задачи и цели исследования. Модель базируется на решении билинейной многошаговой игры качества. Задано: игрок 1 (U)–защитник ИОСУ (ЗИОСУ); игрок 2 (V)– злоумышленник (хакер).Игроки 1 и 2 управляют динамической системой. Система задана системой билинейных дискретных уравнений с зависимыми движениями и соответствующими траекториями, описывающими финансовые стратегии игроков. Необходимо найти множества стратегий игроков, которые предполагают финансировать, соответственно, СКБ и средства преодоления рубежей киберзащиты ИОСУ.

В соответствии с [10–12] две терминальные поверхности – M_0, N_0. Цель ЗИОСУ привести динамическую систему с помощью своих стратегий управления на терминальную поверхность M_0. Сделано допущение, что финансовая стороны нападения на ИОСУ может быть произвольной. Цель атакующих (хакера(ов))привести динамическую систему с помощью своих стратегий управления ФиР, выделяемыми на взлом, на терминальную поверхность N_0, как бы финансово ни действовал ЗИОСУ.

Цель исследования – найти множества начальных состояний объектов и их стратегий, которые позволяют объектам привести систему на ту, или другую поверхность [11]. Решение находится с помощью методов доминирования для бесконечных многошаговых игр [12].

Обзор предшествующих исследований. Ранее в [4, 6, 7] была показана важность проблематики обеспечения надежной и эффективной защиты ИОСУ в условиях стремительной цифровизации и глобализации информационно-коммуникационных систем образовательных учреждений [1]. Разнообразные «дыры» в кибербезопасности периодически обнаруживают даже у крупных университетов и образовательных платформ [6]. Таким образом, задача финансирования СКБ ИОСУ является перманентной. В эпоху глобализации и цифровизациисферы образования, задача оценки эффективности финансирования СКБ ИОСУ становиться одной из приоритетных для служб кибербезопасности и защиты информации современных образовательных учреждений, в частности университетов. Данной тематике исследований, только в последние годы, посвящено большое число публикаций [1–7]. Недостатком многих работ является отсутствие реальных рекомендаций по разработке стратегий финансирования СКБ ИОСУ. В частности, это касается и аспектов, связанных с вопросами моделирования активного финансового противодействия атакующей стороне. В ходе исследования были рассмотрены работы, посвящённые применению различных экспертных [13, 14] и систем поддержки принятия решений [15, 16] для выбора стратегий финансирования СКБ, в частности ИОСУ. Отметим, что многие модели, например, описанные в [13–15], не позволяют находить эффективные рекомендации и стратегии финансирования в СКБ сложных объектов информатизации, в частности ИОСУ. Результаты, приведенные в исследованиях [13–15], не дают однозначного ответа, как ЗИОСУ следует выстроить свою рациональную финансовую стратегию инвестирования в СКБ, в условиях, когда атакующая сторона имеет достаточный для взлома ИОСУ ФиР. При этом в работах [13–15] недостаточно проанализированы ситуации, когда ЗИОСУ не реализовала свой ФиР правильно.

Учитывая дискуссионность положений, изложенных в работах [16–20], релевантной остается проблема дальнейшего развития моделей для ИСППР в задачах финансирования СКБ ИОСУ.

Модели и методы. Безусловно обоим игрокам (ЗИОСУ и хакеру) требуются ФиР для достижения своих целей. Атакующая сторона, например, может использовать стороннее коммерческое программное обеспечение (ПО) для взлома или подкупить персонал, обслуживающий ИОСУ. Будем полагать, что на заданный период времени $\{1,...,T\}$ (T–натуральное число) у ЗИОСУ выделено $de(0)$ ФиР, а у хакера – $ha(0)$. Эти параметры определяют прогнозную, в момент времени $t=0$, величину ФиР, которыми обладают ЗИОСУ и хакер на достижение своих целей. В соответствии [11, 12], принято, что для случая сопоставления решений двух игр – многошаговой и одношаговой мы получим совпадение множеств начальных состояний ФиР ЗИОСУ и хакера со следующим свойством [12, 18].

Свойство 1: множество предпочтительности игрока, исходя из которых он достигает своей цели за T шагов, совпадает со множеством начальных состояний ФиР, из которых он достигает цели за один шаг при применении им оптимальной смешанной стратегии при оптимальном противодействии ему другим игроком в классе смешанных стратегий с вероятностью $1/T$.

В начальный момент времени t ЗИОСУ умножает величину $de(0)$ на коэффициент (темп изменения, роста) $\alpha(t)$ и выбирает величину $u(t)$ $(u(t)\in[0,1])$. Последняя позволит определить долю ФиР ЗИОСУ $\alpha(t)\cdot de(t)$, выделяемую им в момент времени t. Аналогично, в момент времени t хакер умножает величину $ha(t)$ на коэффициент (темп изменения, роста) $\beta(t)$ и выбирает величину $v(t)$ $(v(t)\in[0,1])$. Это определит долю ФиР атакующей стороны (хакера) $\beta(t)\cdot ha(t)$, выделяемую им на взлом ИОСУ.

Введем следующие обозначения: r_1 – коэффициент, показывающий, сколько ФиР потребуется хакеру, чтобы взломать ИОСУ, на защиту которого была израсходована единица ФиР ЗИОСУ; r_2 –коэффициент, показывающий, сколько ФиР потребуется ЗИОСУ, чтобы обезопасить системы ИОСУ, на взлом которых были израсходованы единица ФиРхакера.

Следовательно, с учетом [12, 18, 19], можно описать динамику изменения ФиР ЗИОСУ и атакующих такой системой дискретных уравнений:

$$de(t+1) = \alpha(t)\cdot de(t) - u(t)\cdot\alpha(t)\cdot de(t) - r_2\cdot v(t)\cdot\beta(t)\cdot ha(t); \quad (1)$$

$$ha(t+1) = \beta(t)\cdot ha(t) - v(t)\cdot\beta(t)\cdot ha(t) - r_1\cdot u(t)\cdot\alpha(t)\cdot de(t). \quad (2)$$

В момент времени t должно выполняться одно из условий:

1) $de(t)\geq 0, ha(t)<0$. Если условие 1=*true*, процедура финансирования СКБ ИОСУ завершена. У атакующих не хватило ФиР преодолеть защиту ИОСУ;

2) $de(t)<0, ha(t)\geq 0$. Если условие 2=*true*, то процедура финансирования СКБ ИОСУ завершена. У ЗИОСУ не хватило ФиР для защиты информационно-коммуникационных систем образовательного учреждения.

3) $de(t)<0, ha(t)<0$. Если условие 3=*true*, то процедура финансирования СКБ ИОСУ завершена. Но у ЗИОСУ и у хакера не хватило ФиР достичь своих целей.

4) $de(t)\geq 0, ha(t)\geq 0$. Если условие 4=*true*, то процедура финансирования СКБИОСУ продолжиться далее.

Значения $de(T), ha(T)$ иллюстрируют результаты выделения ФиР на СКБИОСУ.

Выделение ФиР на СКБИОСУ в статье рассмотрено в рамках схемы позиционной многошаговой игры с полной информацией [12].

Процесс выделения ФиР на СКБ ИОСР рассматривается с двух точек зрения (задач):

1) Решение задачи с точки зрения первого игрока-союзника;

2) Решение задачи с точки зрения второго игрока-союзника [11, 12].

Поскольку задачи симметричны, в рамках статьи рассматривается решение задачи с точки зрения первого игрока-союзника.

Обозначим через T^* множество $\{0,1,...,T\}$.

Определение. Чистая стратегия первого игрока-союзника – это функция $u: T^*\cdot[0,1]\cdot[0,1]\to[0,1]$, которая ставит состоянию информации (или позиции) $(t,(de,ha))$ значение $u(t,(de,ha)): 0\leq u(t,(de,ha))\leq 1$.

Следовательно, чистой стратегией первого игрока-союзника будет функция, которая ставит состоянию информации в момент времени t величину $u(t,(de,ha))$. Эта величина определяет долю ФиР ЗИОСУ, которую он планировал потратить на СКБ в момент t.

Допускается, что игрок-противник (хакер) выбирает свое управляющее воздействие и размер своих ФиР, выделяемых на взлом ИОСУ, на основании любой информации.

Определив стратегии в задаче 1, определим множество «предпочтительности» W_1 игрока ЗИОСУ. Тогда, W_1 – множество таких начальных состояний $(de(0), ha(0))$ ФиР ЗИОСУи хакера, которые обладают ниже сформулированным свойством [11].

Свойство 2: для начальных состояний W_1 существует стратегия защитника, которая, для любых реализаций стратегии хакера, «приводит», в один из моментов времени t, состояние системы $(de(0), ha(0))$ в такое, при котором будет выполняться условие (1). При этом, у хакера отсутствует стратегия, которая может «привести» к выполнению условий (2) или (3), в один из предшествующих моментов времени.

Назовем *оптимальной* стратегию (финансовую составляющую) ЗИОСУ, обладающую *свойством 2*.

Решение задачи 1 заключается в нахождении множества предпочтительности ЗИОСУ. Также должны быть определены его оптимальные стратегии. Аналогично ставится задача с точки зрения хакера.

Решение задачи 1 находится с помощью инструментария теории многошаговых игр качества с полной информацией [12, 20–23]. Данный инструментарий позволяет находить решение при любых соотношениях параметров игры.

В статье приведено решение, т.е. множества «предпочтительности» W_1 и оптимальные стратегии $u_*(.,.)$ при всех соотношениях параметров игры.

Случай а) $\alpha \le \beta$.

$$W_1^i = \{\left(de(0), ha(0)\right): k\left(i-1\right)\cdot\beta\cdot ha(0) \le$$

$$r_1\cdot\alpha\cdot de(0) \prec k\left(i-2\right)\cdot\beta\cdot ha(0)\},\ i=1,..$$

$$u_* = \{u_*(0,(de,ha)),...,u_*(i-1,(de,ha))\},$$

$$u_*(t,(de,ha)) = \{[1-(r_2\cdot\beta\cdot ha)/(\alpha\cdot de)]\},$$

при $(de,ha)\in R_+^2,\ \alpha\cdot de > r_2\cdot\beta\cdot ha,$ и не определена – в противном случае; $t = 0,1,...,i-1.$

Обозначим $r_1\cdot r_2 = R_{1,2}, \dfrac{\alpha}{\beta} = \xi.$

Здесь $k(i) = 1+R_{1,2}-(r_1\cdot\alpha\cdot\beta)/(\beta\cdot k(i-1));$

$k_{-1}=0, k_0 = 1+R_{1,2};\ W_1 = \bigcup_{i=1}^{\infty} W_1^i.$

Луч

$$r_1\cdot 2\alpha\cdot de(0) =$$

$$\left\{\left[1+R_{1,2}+\left(\left(1+R_{1,22}\right)^2-4\cdot R_{1,2}\cdot\xi\right)^{0.5}\right]/2\cdot\beta\cdot ha(0)\right\}$$

будет барьером [7]. Барьер – случай, когда из состояний

$$\left(de(0), ha(0)\right): r_1\cdot\alpha\cdot de(0) \le$$

$$\left\{\left[1+R_{1,2}+\left(\left(1+R_{1,2}\right)^2-4\cdot R_{1,2}\cdot\xi\right)^{0.5}\right]/2\cdot\beta\cdot ha(0)\right\}$$

защитник не может достигнуть своей цели в какой-нибудь момент времени.

Случай б) $\alpha \succ \beta,\ R_{1,2}\ge 1.$

В этом случае множество предпочтительности защитника W_1 будет являться объединением конечного числа множеств W_1^i. А именно $(N+2)$ множеств,

где $N: k(i) \succ R_{1,2}\cdot\xi,\ i=0,...,N-1;\ k(N)\le R_{1,2}\cdot\xi,$

$$W_1^i = \{(de(0), ha(0): k\left(i-1\right)\cdot\beta\cdot ha(0) \le$$

$$r_1\cdot\alpha\cdot de(0) \prec k\left(i-2\right)\cdot\beta\cdot ha(0))\},\ i=1,...,N+1;$$

$$W_1^{N+2} = \{(de(0), ha(0): R_{1,2}\cdot\beta\cdot ha(0) \le$$

$$r_1\cdot\alpha\cdot d(0) \prec k\left(N\right)\cdot\beta\cdot ha(0))\}.$$

Тогда, оптимальную финансовую стратегию ЗИОСУ $u_* = (u_*(0,(de,ha),...,u_*(N+1,(de,ha))))$ можно определить так:

$u_*(0,(de,ha)) = \{0,$ при $(x,y)\in R_+^2,\ \alpha\cdot de > r_2\cdot\beta\cdot ha,$ и не определена – в противном случае$\}$, $u_*(t,(de,ha)) = \{[1-(r_2\cdot\beta\cdot ha)/(\alpha\cdot de)],$ при $(de,ha)\in R_+^2,\ \alpha\cdot de > r_2\cdot\beta\cdot ha.$ И не определена – в противном случае; $t = 1,...,N+1\}$.

Случай в) $\alpha \succ \beta,\ R_{1,2}\prec 1.$

В этом случае множество предпочтительности защитника W_1 также будет являться объединением конечного числа множеств W_1^i.

А именно $(N+i_*+2)$ множеств, где $N: k(i)\succ \xi,\ i=0,...,N-1; k(N)\le\xi;$ i_* –минимальное целое неотрицательное число, определяемое неравенством $k(N)\cdot(\beta/\alpha)^{i_*+1}\prec R_{1,2}.$

Тогда

$$W_1^i = \{(de(0), ha(0): k\left(i-1\right)\cdot\beta\cdot ha(0) \le$$

$$r_1\cdot\alpha\cdot de(0) \prec k\left(i-2\right)\cdot\beta\cdot ha(0))\},\ i=1,...,N+1.$$

Если $i_*=0,$ то

$$W_1^i = \{(de(0), ha(0): k\left(i-1\right)\cdot\beta\cdot ha(0) \le$$

$$r_1\cdot\alpha\cdot de(0) \prec k\left(i-2\right)\cdot\beta\cdot ha(0))\},$$

$$i = 1,...,N+1;$$

$$W_1^{N+2} = \{de(0), ha(0): R_{1,2}\cdot\beta\cdot ha(0) \le$$

$$r_1\cdot\alpha\cdot de(0) \prec k\left(N\right)\cdot\beta\cdot ha(0)\}.$$

Выражение для определения оптимальной стратегии ЗИОСУ аналогично случаю б).

Если $i_*>0,$ то

$$W_1^{N+1+j} = \{(de(0), ha(0): k\left(N\right)\cdot\left(\frac{\beta}{\alpha}\right)^j\cdot\beta\cdot ha(0) \le$$

$$r_1\cdot\alpha\cdot de(0) \prec k\left(N\right)\cdot\left(\frac{\beta}{\alpha}\right)^{j-1}\cdot\beta\cdot ha(0))\},$$

$$i = 1,...,i_*;$$

$$W_1^{N+1+i_*} = \{de(0), ha(0): R_{1,2}\cdot\beta\cdot ha(0) \le$$

$$r_1\cdot\alpha\cdot de(0) \prec k\left(N\right)\cdot\left(\frac{\beta}{\alpha}\right)^{i_*}\cdot\beta\cdot ha(0)\}.$$

Тогда, оптимальную стратегию $u_* = (u_*(0,(de,ha)),...,u_*(N+1+i_*,(de,ha)))$ в данном случае определим так:

$u_*(i,(de,ha)) = \{0,$ при $(de,ha)\in R_+^2,\ \alpha\cdot de > r_2\cdot\beta\cdot ha,$ и не определена – в противном случае; $i=0,...,i_*\},$ $u_*(i,(de,ha)) = \{[1-(r_2\cdot\beta\cdot ha)/(\alpha\cdot de)],$ при $(de,ha)\in R_+^2,\ \alpha\cdot de > r_2\cdot\beta\cdot ha,$ $i\ge i_*+1$ и не определена – в противном случае; $t = 1,...,N+1.$

Ранее оговаривалось, что ЗИОСУ обладает ограниченным ФиР. Обозначим максимальное значение ФиРчерез Ω. Тогда множество предпочтительности защитника при таком ограничении W_1^* будет представлять собой пересечение множества W_1 и множества

$$\{(de(0), ha(0)) : (de(0), ha(0)) \in R_+^2,\ de(0) \le \Omega\},$$

т.е. $W_1^* = W_1 \cap \{(de(0), ha(0)) : (de(0), ha(0)) \in R_+^2,\ de(0) \le \Omega\}$.

Аналогичным образом можно найти и множество предпочтительности для хакера. Полагаем при этом, что он обладает ограниченными финансовыми ресурсами.

Таким же образом, решается *задача 2* с точки зрения второго игрока-союзника. Это позволяет представить положительный ортант в плоскости $(de(0), ha(0))$ в виде трех множеств (конусов с вершиной в точке $(0,0)$). Одно множество (конус), примыкающий к оси $0X$, является множеством предпочтительным для ЗИОСУ. Второе множество (конус) является множеством предпочтительным для хакера. Третье множество (конус) является множеством нейтральным, с точки зрения обеих игроков.

Имитационный эксперимент. Имитационные эксперименты выполнялись на платформе ИСППР "SSDMI" [15, 25, 26]. Контрольные расчеты выполнены в пакете Mathcad.

Цели имитационного эксперимента:

1) определить множества стратегий игроков ЗИОСУ и хакера;

2) промоделировать риски, связанные с потерей ФиР игроками.

Результаты имитационных экспериментов показаны в таблице 1 и на рис. 1.

Луч сбалансированности (ЛСБ) на графике показан сплошной линией с круглыми маркерами. На рис. 1 представлены следующие области: под ЛСБ– "предпочтительности" ЗИОСУ; 2) над ЛСБ –"предпочтительности" хакера. Траектория движений ЗИОСУ изображена пунктирной линией с треугольными маркерами. Сплошной линией с квадратными маркерами, показана ограничения на ФиР ЗИОСУ.

Таблица 1

Результаты имитационного эксперимента (ИЭ) по выбору стратегии ЗИОСУ

Номер ИЭ	Результаты моделирования		
	ФиР игроков не ограничен	На ФиР игроков наложены ограничения	
1	(*de*(0),*ha*(0))=(10.0,13.2); (*de*(1),*ha*(1))=(12.0,11.36); (*de*(2),*ha*(2))=(14.0,10.36); (*de*(3),*ha*(3))=(16.0,8.4); (*de*(4),*ha*(4)) = (18.0,6.4).	$\Omega = 14$ Ограничение на ФиР ЗИОСУ	(*de*(0),*ha*(0)) = (7.0,13.0); (*de*(1),*ha*(1))=(8.0,11.0); (*de*(2),*ha*(2)) = (9.0,10.0); (*de*(3),*ha*(3)) = (10.0,8.0); (*de*(4),*ha*(4)) = (11.0,6.0).
2	(*de*(0),*ha*(0))=(5.0,10.0); (*de*(1),*ha*(1))=(4.0,12.0); (*de*(2),*ha*(2))=(3.0,13.0); (*de*(3),*ha*(3))=(2.0,15.0); (*de*(4),*ha*(4))=(1.0,17.0).	$\Omega = 16$ Ограничение на ФиР хакера	(*de*(0),*ha*(0))=(5.0,10.0); (*de*(1),*ha*(1))=(4.0,11.0); (*de*(2),*ha*(2))=(3.0,12.0); (*de*(3),*ha*(3))=(2.0,14.0); (*de*(4),*ha*(4))=(1.0,15.0).
3	(*de*(0),*ha*(0))=(5.0,20.0); (*de*(1),*ha*(1))=(4.0,16.0); (*de*(2),*ha*(2))=(3.0,12.0); (*de*(3),*ha*(3)) = (2.0,8.0), (*de*(4); *ha*(4)) = (1.0,4.0).	$\Omega = 7$ Ограничение на ФиР ЗИОСУ	(*de*(0),*ha*(0)) = (5.0,15.0); (*de*(1),*ha*(1)) = (4.0,12.0);(*de*(2),*ha*(2))=(3.0,9.0), (*de*(3),*hu*(3))=(2.0,6.0);(*de*(4),*ha*(4)) = (1.0,3.0).

С целью проверки адекватности проведенных расчетов, апробация результатов, полученных с помощью ИСППР "SSDMI", выполнена и для реальных проектов в сфере кибербезопасности ИОСУ в Украине («Европейский университет») и Казахстане (Казахский национальный педагогический университет имени Абая).

На рис. 1 рассмотрен случай, в котором игрок защитник ИОСУ, обладает преимуществами в размере начальных финансовых ресурсов. То есть эти ресурсы находятся во множестве предпочтительности ЗИОСУ. Защитник, применяя свою оптимальную стратегию, достигнет своей цели, так как для этого у него достаточно финансовых ресурсов, несмотря на их ограниченность в начальный момент времени. Цель ЗИОСУ– привести состояния системы на «свою» терминальную поверхность [25, 26]. В положительном ортанте на плоскости рассмотрена совокупность лучей, исходящих из точки (0,0). Эти лучи задаются соотношением: $ha = (2.5 - 1/n) \cdot de.$ Эти лучи задают множества предпочтительности первого игрока за *n* шагов.

В процессе реализации имитационного эксперимента, мы показываем, что наша модель, а также ее программная реализация в ИСППР “SSDMI”, способны обеспечить эффективную поддержку принятия решений в сфере финансирования СКБ ИОСУ. Предложенный в работе подход, позволил устранить неопределенность в процессах моделирования финансовых вложений в СКБ ИОСУ.Это выгодно отличает наше исследование от работ других авторов [22, 24, 27, 28-33].

Работа выполнена в рамках грантового финансирования проекта AP05132723 «Разработка адаптивных экспертных систем в области кибербезопасности критически важных объектов информатизации» (Республика Казахстан).

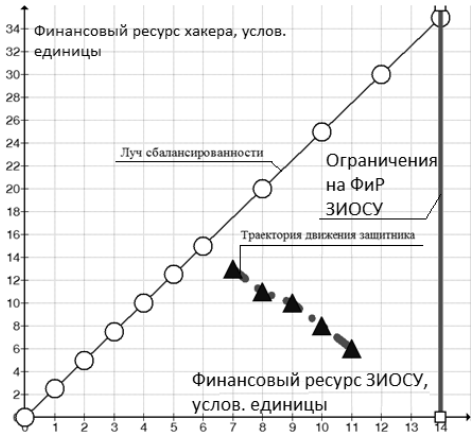

Рис. 1. Области предпочтительности игроков

Выводы. Предложена модель для интелектуализированной системы поддержки принятия решений (ИСППР) в процессе финансирования в средства кибербезопасностии информационно-образовательной среды образовательных учреждений, в частности крупных университетов. Модель основана на теории игр. Разрабатываемая ИСППР позволит конечному пользователю оценивать финансовые стратегии при выпоре направлений инвестирования в СКБ ИОСУ. Научная новизна работы заключается в том, что в отличие от существующих моделей, произведено решение билинейной многошаговой игры качества в классе чистых стратегий, и позволяет производить оценку рисков для игроков, которые, соответственно, представляют стороны защиты и атаки для ИОСУ.

Описаны результаты имитационного эксперимента. В ходе эксперимента учитывались различные соотношения параметров, описывающих процесс финансирования в средства кибербезопасности ИОСУ. На основании результатов имитационного эксперимента и результатов тестирования ИСППР, сделано заключение о рисках утраты финансовых ресурсов для игроков, соответственно на средства киберзащиты и взлома ИОСУ.

ЛИТЕРАТУРА

[1]. Y. Rezgui, M. Adam, "Information security awareness in higher education: An exploratory study", *Computers & Security*, pp. 241-253, 2010.

[2]. N. Sultan, "Cloud computing for education: A new dawn?", *International Journal of Information Management*, pp. 109-116.

[3]. Б. Ахметов, В. Яворский, *Моделирование информационной образовательной среды вуза*, КарГТУ, 2006, 251 с.

[4]. F. Schneider, "Cybersecurity education in universities", *IEEE Security & Privacy* 11.4, pp. 3-4, 2013.

[5]. A. Conklin, "Cyber defense competitions and information security education: An active learning solution for a capstone course", S*ystem Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on. Vol. 9. IEEE*, 2006.

[6]. M. Schuett, M. Rahman, *Information Security Synthesis in Online Universities*, 2011.

[7]. N. Radziwill, M. Benton, *Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management.* [Electronic resource]. Online: https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf, 2017.

[8]. V. Lakhno, Y. Boiko, A. Mishchenko, V. Kozlovskii, O. Pupchenko, "Development of the intelligent decision-making support system to manage cyber protection at the object of informatization", *Eastern-European Journal of Enterprise Technologies*, 2/9 (86), pp. 53-61, 2017.

[9]. S. Ramgovind, M. Eloff, E. Smith, "The management of security in cloud computing", *In Information Security for South Africa (ISSA)*, pp. 1-7, 2010.

[10]. A. Sajid, H. Abbas, K. Saleem, "Cloud-assisted iot-based scada systems security:A review of the state of the art and future challenges", IEEE Access, 4, pp. 1375-1384, 2016.

[11]. V. Malyukov, "A differential game of quality for two groups of objects", *Journal of Applied Mathematics and Mechanics,* Vol. 55, No. 5, pp. 596-606, 1991.

[12]. I. Krass, V. Malyukov, "O sushhestvovanii optimal'-nyh smeshannyh strategij dlja nekotoryh antagonisticheskihigr", *Optimizacija,* pp. 135-146, 1978.
[13]. O. Petrov, B. Borowik, M. Karpinskyy, O. Korchenko, V. Lakhno, *Immune and defensive corporate systems with intellectual identification of threats*, 2016, 222 p.
[14]. K. Goztepe, "Designing Fuzzy Rule Based Expert System for Cyber Security", *International Journal of Information Security Science*, Vol. 1, No 1, pp. 13-19, 2012.
[15]. V. Lakhno, "Development of a support system for managing the cyber security", *Radio Electronics, Computer Science, Control*, No. 2, pp. 109-116, 2017.
[16]. M. Manshaei, Q. Zhu, T. Alpcan, "Game theory meets network security and privacy", *ACM Computing Surveys*, Vol. 45, No. 3, pp. 1-39, 2013.
[17]. N. Ben–Asher, C. Gonzalez, "Effects of cyber security knowledge on attack detection", *Computers in Human Behavior*, Vol. 48, pp. 51-61, 2015.
[18]. J. Grossklags, N. Christin, J. Chuang, "Secure or insure?: a game-theoretic analysis of information security games", *17th international conference on World Wide Web, Beijing, China, 21 – 25 April 2008 : proceedings. New York, ACM*, pp. 209-218, 2008.
[19]. H. Cavusoglu, B. Mishra, S. Raghunathan, "A model for evaluating IT security investments", *Communications of the ACM,* Vol. 47, No. 7, pp. 87-92, 2004.
[20]. A. Fielder, E. Panaousis, P. Malacaria, "Decision support approaches for cyber security investment", *Decision Support Systems*, Vol. 86, pp. 13-23, 2016.
[21]. P. Meland, I. Tondel , B. Solhaug, "Mitigating risk with cyberinsurance", *IEEE Security* & *Privacy,* No. 13(6), pp. 38-43, 2015.
[22]. A. Fielder, S. Konig, E. Panaousis, S. Schauer, S. Rass, *Uncertaintyin Cyber Security Investments*, arXiv preprint arXiv:1712.05893, 2017.
[23]. A. Fielder, E. Panaousis, P. Malacaria, "Game theory meets information security management" *International Information Security Conference, Marrakech, Morroco, 2–4 June 2014 : proceedings, Berlin, Springer*, pp. 15-29, 2014.
[24]. X. Gao, W. Zhong, S. Mei, "Game-theoretic analysis of information sharing and security investment for complementary firms", *Journal of the Operational Research Society*, Vol. 65, No. 11, pp. 1682-1691, 2014.
[25]. V. Malyukov, "Discrete-approximation method for solving a bilinear differential game", *Cybernetics and Systems Analysis*, Vol. 29, No. 6, pp. 879-888, 1993.
[26]. V. Lakhno, V. Malyukov, N.Gerasymchuk, "Development of the decision making support system to control a procedure of financial investment", *Eastern-European Journal of Enterprise Technologies*, Vol. 6, No. 3, pp. 24-41, 2017.
[27]. F. Smeraldi, P. Malacaria, "How to spend it: optimal investment for cyber security", *1st International Workshop on Agents and CyberSecurity, Paris, France, 06–08 May 2014 : proceedings, New York, ACM*, pp. 8, 2014.
[28]. B. Akhmetov, V. Lakhno, Y. Boiko, A. Mishchenko, "Designing a decision support system for the weakly formalized problems in the provision of cybersecurity", *Eastern-European Journal of Enterprise Technologies*, 1(2(85)), pp. 4-15, 2017.
[29]. M. Chronopoulos, E. Panaousis, J. Grossklags, *An options approach to cybersecurity investment*, IEEE Access, 2017.
[30]. S. Rass, S. König, S. Schauer, "Uncertainty in games: Using probability-distributions as payoffs", *In International Conference on Decision and Game Theory for Security,* pp. 346-357, 2015.
[31]. Y. Lee, R. Kauffman, R. Sougstad, "Profit-maximizing firm investments in customer information security", *Decision support systems*, 51(4), pp. 904-920, 2011.
[32]. T. Moore, S. Dynes, F. Chang, *Identifying how firms manage cybersecurity investment.* [Electronic resource]. Online: http://blog. smu. edu/research/ files/ 2015/ 10/SMU-IBM. pdf
[33]. V. Lahno, "Ensuring of information processes' reliability and security in critical application data processing systems", *MEST Journal*, vol. 2, pp. 71-79, 2014.

МОДЕЛЮВАННЯ ПРОЦЕДУРИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ФІНАНСУВАННЯ ЗАСОБІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ОСВІТНЬОГО СЕРЕДОВИЩА УНІВЕРСИТЕТУ

У статті запропонована модель для оцінювання стратегій інвестування в інформаційно-освітнє середовище університету (ІОСУ). Одним з варіантів вирішення подібних завдань, і, зокрема, оцінювання ризиків, пов'язаних з фінансуванням систем захисту інформації та кібербезпеки ОІСУ, є впровадження інтелектуалізованих систем підтримки прийняття рішень (ІСППР). Подібні системи дозволяють менеджменту навчальних закладів приймати раціональні рішення з вкладення фінансових ресурсів у розвиток інструментарію захисту ОІСУ. У статті запропонована модель для ІСППР із використовуванням процедур дискретної оптимізації фінансування систем захисту інформації та кібербезпеки ІОСУ. Відмінною рисою запропонованої моделі від чинних, є припущення обмеженості фінансових ресурсів як сторони захисту ІОСУ, так йнападників. Модель заснована на застосуванні інструментарію теорії багатокрокових ігор. У статті описано рішення білінійної багатокрокової гри якості з залежними рухами в рамках стратегій захисту ІОСУ. Описано результати імітаційного експерименту в рамках вибору фінансових стратегій кіберзахисту ІОСУ. Розробляється інтелектуалізована система підтримки прийняття рішень (ІСППР) дозволить кінцевому користувачеві оцінювати фінансові стратегії при виборі напрямків інвестування у системи інформаційної та кібербезпеки ІОСУ. На відміну від чинних моделей, отримано рішення білінійної багатокрокової гри

якості в класі чистих стратегій. Це дозволяє здійснювати оцінку ризиків для гравців, які, відповідно, представляють сторони захисту та атаки для ІОСУ. В ході імітаційного експерименту були враховані різні співвідношення параметрів, що описують процес фінансування в засоби захисту інформації та кібербезпеки ІОСУ. На підставі результатів імітаційного експерименту і результатів тестування ІСППР, зроблено висновок про ризики втрати фінансових ресурсів для гравців, відповідно на засоби кіберзахисту та зламу ІОСУ.

Ключові слова:кібербезпека, інформаційно-освітнє середовище університету, багатокрокова гра якості, оптимальні стратегії фінансування

MODELING THE DECISION-MAKING PROCEDURE FOR FINANCING CYBERSECURITY FUNDS IN THE INFORMATION AND EDUCATIONAL ENVIRONMENT OF THE UNIVERSITY

The article proposes a model for evaluation of investment strategies in the information and educational environment of the University (IOCC). One of the options for solving such problems, and, in particular, assessing the risks associated with the financing of information security systems and cyber security of IOCC, is the implementation of intelligent decision support systems. Such systems allow the management of educational institutions to make rational decisions on investing financial resources in the development of the IOCC protection tools. The article proposes a model for the IDSP for a discrete procedure for financing the information protection and cyber security systems of the IOCC. Difference of the model from existing ones is the assumption of limited financial resources as the protection side of IOCC and attackers. The model is based on the use of the tools of the theory of multi-step games. The article describes the solution of a bilinear multistep game of quality with dependent motions within the framework of IOCC protection strategies. The results of the simulation experiment within the framework of the choice of financial strategies for cyber defense of IOCC are described. The developed intellectualized decision support system (IDSP) will allow the user to evaluate financial strategies when the investment directions in the information and cyber security information systems of the IOCC are aligned. Unlike existing models, a bilinear multistep game of quality in a class of pure strategies has been solved, and it makes it possible to assess the risks for players who accordingly represent the sides of defense and attack for IOCC. Various ratios of the parameters describing the financing process in the information protection and cyber security protection facilities of the IOCC were taken into account. In the course of the simulation experiment based on the results of the simulation experiment and the test results of the IDSP, a conclusion was made about the risks of loss of financial resources for players, respectively, by means of cyber defense and hacking the IOCC.

Key words: cybersecurity, information and educational environment of the university, multi-stage quality play, optimal financing strategies.

Кыдыралина Лазат Муктаровна, докторант, Казахский национальный педагогический университет имени Абая, г.Алматы, Казахстан.
E-mail: Lazat_75@mail.ru.
Кидираліна Лазат Муктаровна, докторант, Казахський національний педагогічний університет імені Абая, м.Алмати, Казахстан.
Kydyralina Lazat, doctoral, Kazakh National Pedagogical University named after Abay**,** Almaty, Kazakhstan.

Ахметов Бахытжан Сражатдинович, директор Центра повышения квалификации и дистанционного образования, Казахский национальный педагогический университет имени Абая, доктор технических наук, профессор, г.Алматы, Казахстан.
E-mail: bakhytzhan.akhmetov.54@mail.ru.
Ахметов Бахитжан Сражатдіновіч, директор Центру підвищення кваліфікації та дистанційної освіти, Казахський національний педагогічний університет імені Абая, доктор технічних наук, професор, м.Алмати, Казахстан.
Akhmetov Bakhytzhan, director of the Center for advanced studies and distance education, Kazakh National Pedagogical University named after Abay, Almaty, Kazakhstan.

Лахно Валерий Анатольевич, доктор технических наук, профессор, заведующий кафедрой кибербезопасности и управления защитой информационных систем, Европейский университет, г. Киев, Украина.
E-mail: Valss21@i.ua.
Лахно Валерій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та управління захистом інформаційних систем, Європейський університет, м Київ, Україна.
Lakhno Valeri, doctor of Engineering; professor, head of the department cyber security and managements of protection of information systems, European university, Kiev, Ukraine.