Теоретико-игровые подходы в анализе стратегий защиты корпоративных информационных систем

Павел Конюховский, Андрей Шабалин

***Аннотация* — Работа посвящена проблемам применения моделей и методов теории стратегических игр для описания процессов функционирования информационных систем. Предложена биматричная игровая модель взаимодействия информационной системы с агрессивной внешней средой. В данной игре в возможные стратегии защиты информационной системы формализованы до набора действий: приоритет оборудования, приоритет стороннего программного обеспечения, приоритет собственного программного обеспечения, ставка на внешнюю экспертизу, ставка на жёсткий режим безопасности. В качестве возможных стратегий атакующей стороны рассматриваются целевая продолжительная атака, случайный поиск, инсайдерская атака, взлом смежной системы. В предположении возможности построения системы полезностей игры на основе экспертных оценок продемонстрированы возможности её анализа с использованием концепции равновесия по Нэшу, а также его частного случая– «равновесия дрожащей руки».**

Отдельно в работе рассматриваются возможные варианты трансформации базовой статической биматричной модели в повторяющуюся игру, а также в динамическую игру с неполной информацией. Последнее направление представляет особый интерес, так как более адекватно реалиям сферы защиты информации и поддержания устойчивого функционирования информационных систем. В частности, продемонстрирована возможность применения концепции совершенного равновесия по Байесу–Нэшу для выработки систематической политики защиты. Перспективным направлением имплементация предлагаемых моделей является их комплексное использование совместно с системами (алгоритмами) сценарного прогнозирования.

***Ключевые слова*—информационная система, безопасность, устойчивость, теоретико-игровые модели безопасности информационных систем, стратегические игры, байесовы игры.**

I. Введение

Вопросы развития систем электронного управления, электронного участия граждан во взаимодействии с органами государственного управления приобретают особую значимость в эпоху глобальной цифровой трансформации.

Возросла весомость и значимость проблем устойчивости и безопасности программно-технических комплексов. В исследованиях данных проблем особое значение приобретает понимание природы угроз безопасности информационных систем. При их рассмотрении следует обратить внимание на следующие факторы.

- Следствием повышения функциональных возможностей информационных систем стало возрастание объёма потенциального ущерба в случае их взлома или выведения из строя.
- Обратной стороной накопления опыта эксплуатации становится накопление опыта атак.
- Нарастание сложности и масштабности систем объективно ведёт к росту потенциальных «слабых мест» и уязвимостей.
- Многократное увеличение количества пользователей предоставляет дополнительную информацию и возможности для «недобросовестных пользователей». В частности, ощутимо расширились возможности маскировки атак ввиду осложнения процедур локализации их источников. В этой связи необходимо особо подчеркнуть актуальность дилеммы выбора между масштабом, с одной стороны, и управляемостью (контролируемостью, обозримостью) информационной системы, с другой.
- Эффект «автогенерации оппозиции» – по мере жизненного цикла системы естественных образом создаётся кадровый ресурс для групп её антагонистов, готовых поддержать деструктивные действия по отношению к ней. Как правило, это бывшие разработчики или сотрудники, а также IT-специалисты, не нашедшие возможностей для самореализации в легальных проектах.
- «Эндогенные угрозы», то есть угрозы выхода информационных систем из под контроля со стороны управляющего персонала. Последнее может происходить по причинам отсутствия у персонала адекватного представления о логике, алгоритмах, правилах функционирования программно-технических комплексов. Прежде всего в силу их «необозримой сложности». Также причиной подобных явлений может стать несогласованность прав и компетенций персонала на разных уровнях управления информационными

Статья получена 20 октября.

П.В. Конюховский, Российский государственный педагогический университет им. А.И.Герцена (Санкт-Петербург), Северо-Западный институт управления РАНХиГС (Санкт-Петербург) (e-mail: kon_pv@mail,ru).

А.А. Шабалин, аспирант кафедры бизнес-информатики, Северо-Западный институт управления РАНХиГС (Санкт-Петербург) (e-mail: ashabalin750@gmail.com).

системами. Иногда угрозы подобной природы получают громкое и эффектное наименование «восстания машин». Наверное, более правильной и адекватной формулировкой была бы «утрата управления машинами».

— «Новые экзогенные угрозы». Двадцатые годы XXI-го века ознаменовались ярко выраженными контр-глобализационными трендами и тенденциями к сегментации мировых экономических, социальных и политических систем. В настоящий момент мы наблюдаем формирование локальных союзов и коалиций, характеризующихся объективными конфликтами интересов. Это не может не получить отражения на уровне взаимоотношения разработчиков программно-технических систем и их потенциальных потребителей. Действительно, так или иначе они аффилированы с соответствующими конкурирующими центрами силы.

В современных условиях адекватными и конструктивными инструментами представления процессов функционирования информационных систем становятся модели и методы теории игр.

На первичном (поверхностном) уровне эта адекватность определяется тем, что рассматриваются именно методы принятия решений в условиях неопределённости (а не риска). Действительно в случае защиты информационных систем мы имеем дело с противостоянием сознательно действующему оппоненту.

На более глубинном уровне речь идёт о сложных (комплексных) взаимосвязях инфосистем с внешней средой. Под внешней средой подразумеваются как клиентское сообщество, так и конкурирующие системы.

В последние годы в число активно развивающихся направлений научных и научно-практических исследований вошла проблематика электронного участия граждан в процессах местного и государственного управления, см., например, [8]. В данном случае целесообразно упомянуть содержательную взаимосвязь данных вопросов с проблематикой доверия населения (граждан) к системам поддержки государственного управления, задачам эффективного электронного участия. Зачастую электронного участия, недоверие к инструментам цифрового управления вызывается не столько подозрениями относительно их технических и конструктивных возможностям или неудовлетворённостью интерфейсными решениями, сколько явным или неявным ощущением отчуждённости от процессов, поддерживаемыми информационными комплексами.

Цифровизация, рассматриваемая с точки зрения её социально-экономических и социально-политических аспектов, в первую очередь значима и знаменательна тем, что обеспечивает для относительного меньшинства возможности контроля за остальными членами общества, изолированного от доступа к информационным массивам и инструментам работы с ними.

Отчасти прослеживается аналогия с чертами феодального строя. Информация играет роль земли, доступ к инструментам работы с информацией – право на владение оружием. Разумеется, любые аналогии такого рода относительны и дискуссионны. Однако нельзя отрицать наличие в них содержательных составляющих.

Дополнительную остроту в проблематику безопасности и надёжности информационных систем вносят радикальные изменения в системе международных политико-экономических отношений, сдвиги весов, значимости и влияния мировых «центров силы». Кластеризация и сегментация мира актуализировала проблемы технологической зависимости и независимости, выдвинула на передний план понятия цифрового суверенитета и, соответственно, цифрового вассалитета. Последний предполагает зависимость на базовом уровне информационных систем государств и корпораций от внешних по отношению к ним сил, то есть производителей технического и программного обеспечения, контролируемых другими государствами или корпорациями.

II. Предшествующие исследования и смежная проблематика

Несмотря на то, что теоретико-игровые подходы не являются мейнстримом в научных и научно-практических исследованиях проблем защищённости информационных систем, к настоящему времени вышла достаточно представительная серия публикаций, посвящённых данной проблематике.

Среди работ, наиболее близких по методам и подходам к настоящей статье, следует упомянуть публикацию [4]. В ней предлагается представление системы взаимодействия стороны, стороны, защищающей инфокоммуникационный объект, (игрок А) и атакующей стороны (игрок В) в форме матричной игры. Игрок А имеет семь стратегий защиты: физическая защита, техническая защита, криптографическая защита, защита на уровне ПО, защита на уровне «железа», «бумажная безопасность», сетевая защита. Игроку В вменяется пять стратегий (вариантов) нападения: отгадывание пароля, заражение системы вирусом, несанкционированный доступ, заражение шпионским программным обеспечение, DDoS атака. Далее используются классические методы анализа матричных игр – нахождение седловой точки, решение в смешанных стратегиях, решения на основе критериев Вальда, Сэвиджа, Гурвица. По результатам данных исследований автором делается вывод о важности теоретико-игровых подходов для лиц, принимающих решение при выборе стратегий защиты инфокоммуникационных объектов.

Статья [9] посвящена схожему подходу. Участниками конфликта выступают руководство предприятия (сторона информационной защиты) и злоумышленники (атакующую сторона). Собственно, конфликт предлагается моделировать с помощью матричной игры. На основании игровой модели предполагается решать

задачи распределения мощностей системы защиты, максимизирующие эффекты отражения атаки.

В статье [7] предлагается теоретико-игровая модель с n игроками, которые группируются в соответствии с определёнными иерархическими принципами. При рассмотрении задач информационной безопасности группа нулевого уровня формируется из пользователей информационной системы, системы защиты информации и нарушителей информационной безопасности. В качестве ресурса выступает временные и вычислительные ресурсы информационной системы.

Серьёзное внимание проблематике формализации стратегий в моделях противодействия нарушителям информационной безопасности уделяется в [1]. В статье систематизируются угрозы и соответствующие им уязвимости. В дальнейшем на этой основе формулируется оригинальная методика сопоставления классов нарушителей доступных видов уязвимостей, что, в свою очередь, позволяет построить систему количественных оценок (показателей) в соответствии с принципом «чем более быстрым и опасным является проникновение нарушителя, тем большее числовое значение присваивается показателю». По мнению авторов разработанные ими формализованные модельные конструкции могут быть положены в основу программного обеспечения, решающего задачи автоматизации защиты.

В работе [14] предлагаются теоретико-игровые подходы к управлению киберфизическими системами (CPS). Особенностью таких систем является повышенный риск внешних атак. В подобных ситуациях особую актуальность приобретает комплексное сочетание теоретико-игровых методов и т.н. «мультиагентного» обучения.

В статье [15] рассмотрено применение концепции равновесия Байеса-Нэша при моделировании процессов защиты информационных объектов. Авторы конструируют функциональную зависимость, позволяющую сформулировать задачу поиска равновесия между оптимальными стратегиями защиты и нападения. Также в данной работе предлагается прикладная модель, моделирующая ситуацию нападения и защиты.

В контексте обзора теоретико-игровых работ будет полезным упомянуть публикации, относящиеся к смежным направлениям. В частности, к оптимизационным подходам. В статье [10] предлагается модель управления рисками информационной безопасности, сводящаяся к задаче линейного программирования. В качестве переменных выступают затраты на защиту от различных угроз (рассматривается конечное число угроз). Целью является минимизация суммарных рисков. Целевая функция представляет собой сумму произведений вероятностей рисков угроз на затраты на противодействие им. Нельзя не обратить внимание на неоднозначность и дискуссионность подобной концепции. Также в работе формулируется дискретная версия оптимизационной модели, содержательно аналогичная т.н. задаче о ранце.

Говоря о современных или относительно современных методах анализа проблем информационной безопасности, не следует игнорировать и те методы, которые эффективно и конструктивно проявили себя в прошлом. При этом их потенциал далеко не исчерпан. В этом ряду можно отметить методы принятия решений в условиях риска и неопределённости. Они, в частности, получили плодотворное развитие в работах [11, 12, 13]. В них предложен фундаментальный теоретический аппарат принятия решений в условиях неполной, неточной, нечисловой информации (т.н. ННН-информации). На базе этого инструментария могут сформированы алгоритмы построения интегрированных сводных показателей, что представляет несомненный интерес с точки зрения задач оценивания результатов процессов класса «нападение–защита».

III. Базовая модель взаимодействия информационной системы с агрессивной внешней средой

Последовательно поясним идейную составляющую предлагаемых далее теоретико-игровых моделей, описывающих логику поведения информационной системы, выступающей в роли объекта потенциальных атак.

На начальном уровне процессы обеспечения безопасности информационной системы, выработки стратегий её поведения могут быть формализованы в виде абстрактной биматричной игры.

В качестве игрока I выступает собственно информационная система. Игрок II олицетворяет внешние угрозы. Разумеется, подобное интегрированное представление является серьёзным упрощением реально существующих угроз и источников деструкции. Однако с точки зрения логики поведения лиц, ответственных за работу информационной системы, такой подход обладает рядом очевидных конструктивных достоинств. Действительно, по факту (за редким исключением) потенциальные источники угроз с позиций самой системы допускают формализацию в виде некоторой анонимной «имперсонализированной силы». В дальнейшем для краткого наименования предлагаемой игровой модели будет использоваться аббревиатура БИМВИСАС – Биматричная Игровая Модель Взаимодействия Информационной Системы с Агрессивной Внешней Средой.

Формальная схема предлагаемой биматричной игры представлена в табл. 1. Строки таблицы соответствуют стратегиям (действиям) игрока I $(s_i^1, i \in \{1, \dots, m\})$, столбцы – стратегиям игрока II $\left(s_j^2, j \in \{1, \dots, n\}\right)$. Клетки таблицы отображают полезности (платежи, выигрыши/проигрыши) игроков – $u_{i,j}^1$, $u_{i,j}^2$. – в зависимости от ситуаций в чистых стратегиях (игрок I выбирает свою стратегию s_i^1, а игрок II, соответственно, его стратегию s_j^2).

В качестве основных направлений анализа БИМВИСАС могут быть предложены:

— определение равновесий по Нэшу в чистых стратегиях;

— определение равновесий по Нэшу в смешанных стратегиях;
— анализ свойств устойчивости/неустойчивости равновесий;
— применение различных концепций очищения равновесий, в частности анализ с позиций «равновесия дрожащей руки» [16].

Разумеется, в случае защиты реальных информационных систем алгоритмы, методы и стратегии их защиты отличаются чрезвычайным разнообразием. Более того, важнейшим критерием успешности данного процесса является нахождение инновационных, ранее неизвестных решений, которые не смогут предвидеть потенциальные «взломщики». Однако в случае упрощённой игровой модели с точки зрения прикладных реалий разумно ограничиться выбором из набора типичных («классических») методов.

Пример конкретной реализации БИМВИСАС дан в табл. 2.

В рамках рассматриваемой игровой модели в качестве стратегий игрока I (способов защиты) рассматриваются:

— A – приоритет оборудования – основной упор защищающейся стороной делается на техническое обеспечение;
— B – приоритет ПО (стороннее ПО) – защищающаяся сторона делает ставку на стороннее программное обеспечение;
— C – приоритет ПО (собственное) – защищающаяся сторона делает ставку на разработку собственного программного обеспечения;
— D – сторонний аудит – ставка на внешнюю экспертизу;
— E – жёсткий режим безопасности – ставка на т.н. «политики безопасности».

Множество стратегий игрока II (атакующей внешней среды) было ограничено набором:

— X – целевая продолжительная атака;
— Y – случайный поиск жертвы;
— Z – инсайдерская атака;
— W – взлом смежной системы.

Таблица 1. Биматричная игровая модель взаимодействия информационной системы с агрессивной внешней средой

			ИГРОК II –Внешняя атакуюшая среда				
			Стратегия 1	…	Стратегия j	…	Стратегия n
			s_1^2	…	s_j^2		s_n^2
ИГРОК I –Информационная система	Стратегия 1	s_1^1	$u_{1,1}^2$ $u_{1,1}^1$	…	$u_{1,j}^2$ $u_{1,j}^1$	…	$u_{1,n}^2$ $u_{1,n}^1$
	…	…	…	…	…	…	…
	Стратегия i	s_i^1	$u_{i,1}^2$ $u_{i,1}^1$	…	$u_{i,j}^2$ $u_{i,j}^1$	…	$u_{i,n}^2$ $u_{i,n}^1$
	…	…	…	…	…	…	…
	Стратегия m	s_m^1	$u_{m,1}^2$ $u_{m,1}^1$	… …	$u_{m,j}^2$ $u_{m,j}^1$	… …	$u_{m,n}^2$ $u_{m,n}^1$

Источник: составлено авторами

Таблица 2. Пример биматричной игровой модели взаимодействия информационной системы агрессивной внешней средой

			ИГРОК II –Внешняя атакуюшая среда			
			Целевая продолжительная атака	Случайный поиск	Инсайдерская атака внутренняя компрометац.	Взлом смежной системы
			X	Y	Z	W
ИГРОК I –Информационная система	Приоритет оборудования	A	−2 4	4 1	1 −5	−2 5
	Стороннее ПО	B	5 5	4 5	4 3	3 −3
	Собственное ПО	C	2 −5	−3 −3	4 −1	−5 4
	Сторонний аудит	D	−3 −4	−1 −5	−4 −4	0 −5
	Жёсткий режим	E	−3 2	−4 4	−3 5	−4 0

Источник: составлено авторами

Таким образом, игровая модель имеет 20 ситуаций в чистых стратегиях. Полезности участников $\left(u_{i,j}^1, u_{i,j}^2\right)$ по аналогии с табл. 1 расположены в клетках – левый нижний угол полезность игрока I, правый верхний – полезность игрока II.

Значения полезностей варьируются в интервале от -5 (наихудший исход для игрока) до $+5$ (наилучший исход). Они представляют собой нормализованные экспертные оценки.

В биматричной игре, задаваемой табл. 2, существуют два равновесия по Нэшу в чистых стратегиях (выделены цветом). Это ситуации:

— {«Стороннее ПО»; «Целевая продолжительная атака»};
— {«Жёсткий режим»; «Инсайдерская атака»}.

Ценность этого результата заключается не столько в его адекватности реалиям современной информационной среды, сколько в том, что он правдоподобно отражает устойчивые мнения профессиональной среды о свойствах и закономерностях информационных противостояний.

Более содержательным с точки зрения выявления закономерностей противостояния обороняющейся и атакующей сторон представляется исследование БИМВИСАС на предмет существования равновесий в смешанных стратегиях.

В случае биматричных игр это относительно несложная в математическом плане задача. Она предполагает нахождение векторов смешанных стратегий

— $\mathbf{p}^* = (p_1^*, \dots, p_i^*, \dots, p_m^*)$ – игрока I;
— $\mathbf{q}^* = (q_1^*, \dots, q_j^*, \dots, q_n^*)$ – игрока II,

которые удовлетворяют условиям

$(\forall\, s_i^1 : p_i^* > 0)\ \ u_1(\mathbf{p}^*, \mathbf{q}^*) = u_1(s_i^1, \mathbf{q}^*),$
$(\forall\, s_i^1 : p_i^* = 0)\ \ u_1(\mathbf{p}^*, \mathbf{q}^*) \geq u_1(s_i^1, \mathbf{q}^*),$
$\left(\forall\, s_j^2 : q_j^* > 0\right)\ \ u_2(\mathbf{p}^*, \mathbf{q}^*) = u_2\left(\mathbf{p}^*, s_j^2\right),$
$\left(\forall\, s_j^2 : q_j^* = 0\right)\ u_2(\mathbf{p}^*, \mathbf{q}^*) \geq u_2\left(\mathbf{p}^*, s_j^2\right),$

где

$u_1(\mathbf{p}^*, \mathbf{q}^*), u_2(\mathbf{p}^*, \mathbf{q}^*)$ – полезности игроков I и II в ситуации равновесия в смешанных стратегиях;

$u_1(s_i^1, \mathbf{q}^*)$ – полезность игрока I в ситуации, когда он играет свою чистую стратегию s_i^1, а его оппонент (игрок II) играет равновесную смешанную стратегию $\mathbf{q}^*$;

$u_2\left(\mathbf{p}^*, s_j^2\right)$ – полезность игрока II в ситуации, когда он играет свою чистую стратегию s_j^2, а его оппонент (игрок I) играет равновесную смешанную стратегию $\mathbf{p}^*$.

Конструктивность и плодотворность равновесного решения в смешанных стратегия в первую очередь определяется тем, что оно может быть имплементировано как некоторый устойчивый (регулярно воспроизводимый) стратегический выбор сторон. Одновременно не следует игнорировать и того удручающего обстоятельства, что равновесий в смешанных стратегиях может быть очень много (в том

числе, и бесконечно много). Это, в свою очередь, порождает естественный вопрос «к какому именно из них будет сходиться поведение игроков?»

Для преодоления подобных трудностей в теории игр применяются методы очищения равновесия. К настоящему моменту их существует достаточно много. В частности, применительно к БИМВИСАС заслуживает внимание концепция «равновесия дрожащей руки», восходящая к работам [16].

Основным свойством равновесия дрожащей руки является свойство сохранения устойчивости при незначительных отклонениях игроков от равновесных стратегий. Под термином «дрожащая рука» понимается ситуация, в которой один из игроков по ошибке «нажмёт неверную кнопку».

Несложно заметить, что равновесие {«**Стороннее ПО**»; «**Целевая продолжительная атака**»} обладает свойствами равновесия дрожащей руки. Действительно, если допустить, что игрок I отклонится и вместо равновесной стратегии «**Стороннее ПО**» сыграет некоторую смешанную стратегию $\mathbf{p}' = \left(\frac{\varepsilon}{4}, 1-\varepsilon, \frac{\varepsilon}{4}, \frac{\varepsilon}{4}\right)$, где ε –некоторая малое число (вероятность отклонения от равновесной стратегии), то игрока II не возникнет стимулов к отклонению от его равновесной стратегии «**Целевая продолжительная атака**»:

$$u_2(\mathbf{p}', s_{\mathrm{X}}^1) > \begin{cases} u_2(\mathbf{p}', s_{\mathrm{Y}}^1), \\ u_2(\mathbf{p}', s_{\mathrm{Z}}^1), \\ u_2(\mathbf{p}', s_{\mathrm{W}}^1) \end{cases}$$

при малых ε.

Равновесие {«**Жёсткий режим**»; «**Инсайдерская атака**»} также является равновесием дрожащей руки. При этом целесообразно обратить внимание на неравнозначность полезностей второго игрока в первом и втором равновесии. Вполне вероятно, что к осмысленности равновесия {«**Жёсткий режим**»; «**Инсайдерская атака**»} могут возникнуть вопросы. Его оправданием может служить, тот «рациональный довод», что при жёсткой политики безопасности у атакующей стороны нет лучшего решения, чем, всё-таки, пытаться взломать систему изнутри

IV. Развитие базовой теоретико-игровой модели

Конструктивные свойства БИМВИСАС обеспечивают технологические возможности её развития.

В первую очередь она может быть имплементирована в повторяющуюся игру. На каждом этапе такой игры рассматривается противостояние игроков – атака и отражение. Результаты розыгрыша очередного этапа дают информацию для последующих этапов. Важным качеством повторяющихся игр является то, что в них могут возникать совершенные подыгровые равновесия, не сводящиеся к повторению равновесия базовой игры.

Ещё одним вариантом развития БИМВИСАС может стать её трансформация в динамическую игру с неполной информацией (динамическую байесову игру).

Принципиальная схема такой игры показана на рис. 1. Выделяются три этапа.

(1) Игрок II – атакующая сторона (в целях преемственности изложения мы сохраняем предшествующие обозначения) принимает предварительное решение о типе нападения (по существу, на этом шаге моделируется сложившаяся система «типичных» угроз).

(2) Игрок I – защищающаяся сторона принимает решение о способе защиты. При этом он не обладает полной информацией о выборе оппонента, а руководствуется только своими представлениями о нём. Факт неразличимости для игрока I множества вершин, из которых им совершается ход, моделируется с помощью т.н. информационного множества. На схеме (рис. 1) информационное множество показано в виде пунктирной фигуры («прямоугольник с закруглёнными углами»). Система представлений моделируется с помощью вероятностного распределения, заданного на вершинах, принадлежащих информационному множеству:

θ_{X}^1 – оценка вероятности игроком I того, что игрок II выбрал способ атаки **X**;

θ_{Y}^1 – оценка вероятности игроком I того, что игрок II выбрал способ атаки **Y** и т.д.,

где $\theta_{\mathrm{X}}^1, \theta_{\mathrm{Y}}^1, \theta_{\mathrm{Z}}^1, \theta_{\mathrm{W}}^1 \geq 0$, $\theta_{\mathrm{X}}^1 + \theta_{\mathrm{Y}}^1 + \theta_{\mathrm{Z}}^1 + \theta_{\mathrm{W}}^1 = 1$.

(3) Игрок II совершает фактическую атаку. При этом он имеет полную информацию о том, какой предварительный сигнал был им послан на шаге 1. Однако обладает исключительном системой представлений (а не полной информацией) о способе защиты, выбранном игроком I на шаге 2. Таким образом, игрок 2 совершает свой ход в одном из пяти информационных множеств с системами представлений:

$\theta_{X,A}^2, \theta_{X,B}^2, \theta_{X,C}^2, \theta_{X,D}^2, \theta_{X,E}^2 \geq 0$,
$\theta_{X,A}^2 + \theta_{X,B}^2 + \theta_{X,C}^2 + \theta_{X,D}^2 + \theta_{X,E}^2 = 1$;
$\theta_{Y,A}^2, \theta_{Y,B}^2, \theta_{Y,C}^2, \theta_{Y,D}^2, \theta_{Y,E}^2 \geq 0$,
$\theta_{\mathrm{Y,A}}^2 + \theta_{Y,B}^2 + \theta_{Y,C}^2 + \theta_{Y,D}^2 + \theta_{Y,E}^2 = 1$;

и т.д.

По результатам предпринятой последовательности действий игроки получают полезности (платежи) $u_1(\circ), u_2(\circ))$.

Основным предметом исследования в подобных игровых моделях является совершенное равновесие по Байесу-Нэшу. В данном случае мы воздержимся от формулировки его строго определения, что было бы более уместным в соответствующем учебном курсе по динамическим байесовым играм. Подчеркнём лишь один принципиальный аспект. В основе концепции совершенного равновесия по Байесу-Нэшу лежит последовательная рациональность действий игроков с учётом имеющихся у них представлений. Таким образом равновесие по Байесу-Нэшу – это именно комплекс из действий и представлений (вероятностных распределений). Данный класс равновесий учитывает как предысторию игры, так и представления участников игры об этой предыстории. В задачах анализа безопасности и устойчивости информационных систем это свойство совершенного байесова равновесия играет чрезвычайно важную и плодотворную роль. Действительно, при организации стратегий защиты/нападения нужно ориентироваться не только на

собственное мнение об оппоненте, но и пытаться предвидеть (прогнозировать, предугадать) его мнение о тебе.

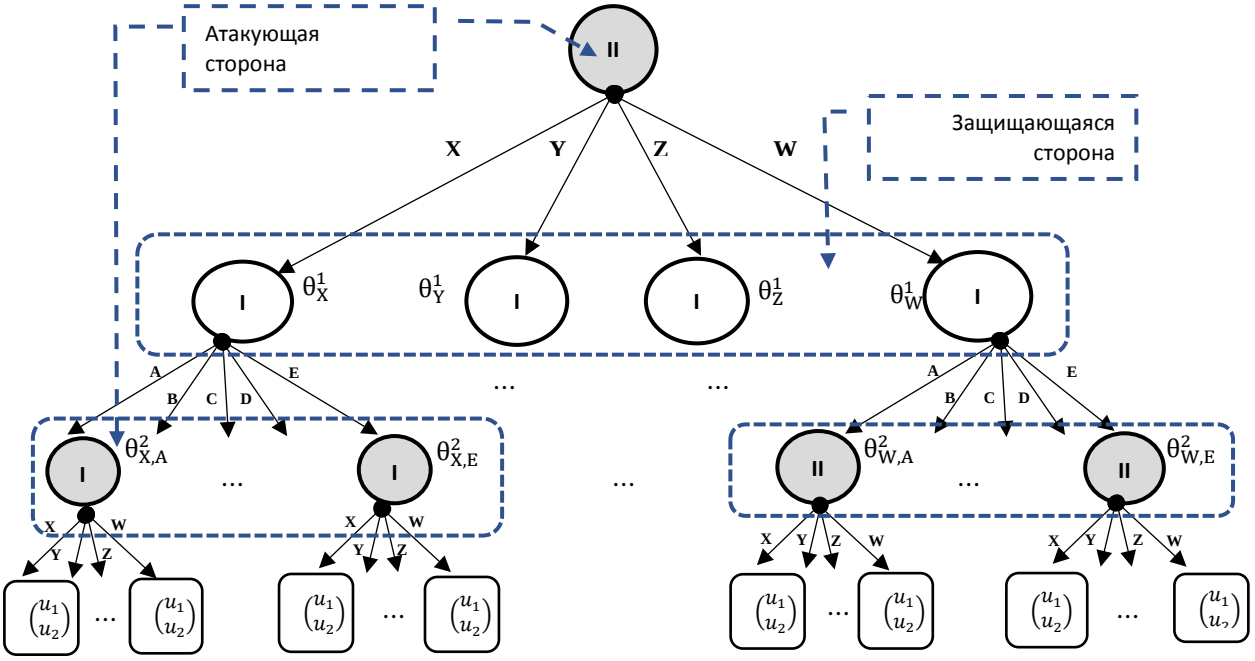

Рис. 1. Модель взаимодействия информационной систем с агрессивной внешней средой на основе динамической байесовой игры

V. Возможные прикладные имплементации

Адекватно конструктивным и перспективным направлением практической имплементации теоретико-игровых моделей взаимодействия информационной системы с агрессивной внешней средой являются задачи сценарного прогнозирования (сценарно-прогностического анализа). Проблематика развития данного направления применительно к процессам цифровой трансформации финансовой сферы затрагивалась, например, в [2, 3, 5].

Принципиальная схема сценарно-прогностического подхода представлена на рис. 2. Проблематика применения подобных подходов в сфере анализа процессов эволюции цифровых валютных инструментов достаточно подробно рассмотрена в [6]. Сценарно-прогностические модели предполагают математическую формализацию исследуемой (анализируемой) последовательности событий (сценария) в виде древовидного графа. Вершины графа соответствуют качественным состояниям, дуги – вариантам перехода к следующим состояниям. Рис. 2 отражает сценарий, при котором моделируемая система может перейти из исходного состояния (0) к состояниям 1, 2 или 3. В свою очередь из состояния 1 возможны переходы к состояниям С. 1.1, С. 1.2, С. 1.3, из состояния 2 к состояниям С. 2.1, С. 2.2., С. 2.3 и т.д. В общем случае количество вариантов перехода для разных вершин сценарного дерево может быть различаться.

Каждой из дуг ставится в соответствие некоторая вероятность (оценка) реализации именно этой ветви сценария в случае достижения вершины инцидентной данной дуге. Таким образом, мы можем получить вероятности реализации всех оконечных вершин сценарного графа.

Конкретные значения вероятностей могут быть построены на базе экспертных оценок. При этом непосредственно эксперту может предлагаться осуществить оценку исходов для той или иной вершины исключительно на качественном (вербальном) уровне. В формате «если развитие событий приведёт к ситуации, которая соответствует текущей вершине, то последующий переход по дуге a более вероятен (логичен, ожидаем) по сравнению с переходом по дуге b, ну а переход по дуге предельно c маловероятен». На текущий момент разработан мощный и эффективный математический аппарат, с помощью которого может быть решена задача квантификации неточных и нечётких экспертных оценок, см., например, [11, 13].

В роли экспертов могут выступать специалисты в соответствующей предметной области, так и формальные модели и прогностические алгоритмы.

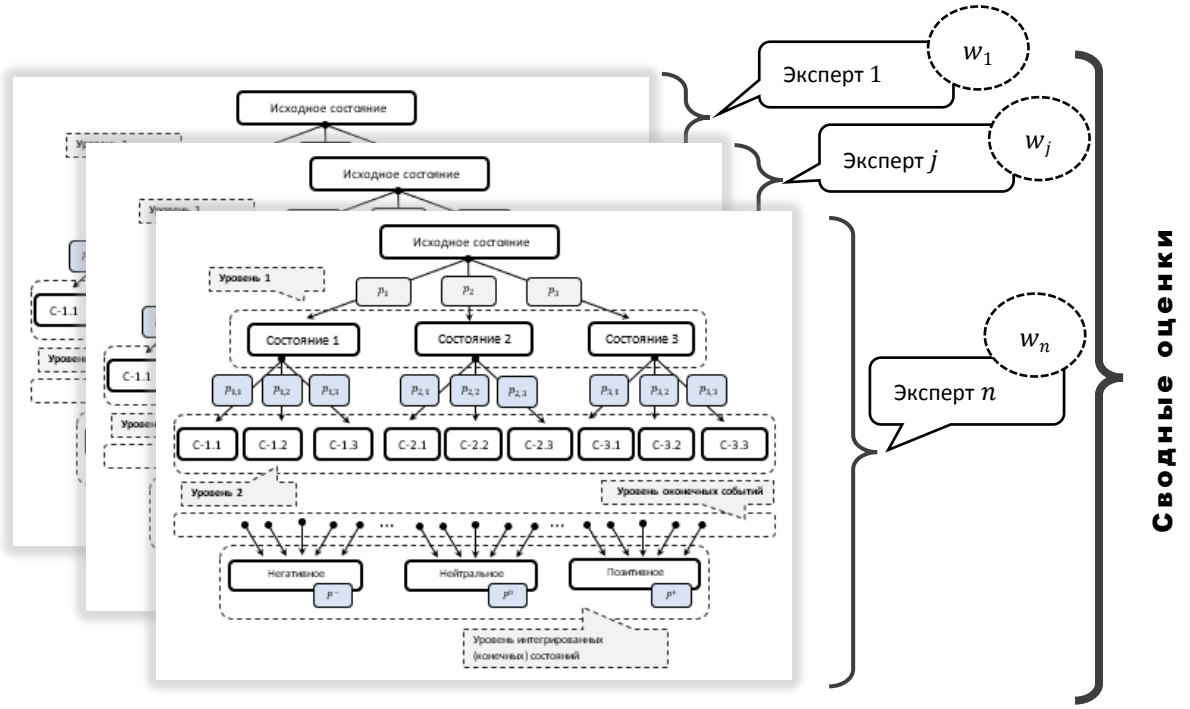

Рис. 2. Процедура сценарно-прогностического анализа (принципиальная схема)

В силу значительности числа оконечных вершин «естественным» и ожидаемым оказывается результат, в соответствии с которым каждая отдельная терминальная вершина характеризуется малой вероятностью. Однако «точечные» состояния могут объединены в содержательно-осмысленные *интегрированные конечные состояния*, вероятности которых определяются как суммы вероятностей терминальных вершин.

Дальнейшая реализация процедуры сценарно-прогностического анализа предполагает организацию серии альтернативных экспертных оценок сценарного графа. Полученные (от каждого из экспертов) значения вероятностей вновь интегрируются на следующем уровне.

Интеграция идёт по множеству всех неоконечных вершин. Такой порядок позволяет работать с набором неполных (асимметричных) экспертных оценок, то есть в тех случаях, когда некоторые эксперты оценивают только отдельные фрагменты сценарного дерева.

При расчёте сводных вероятностей эксперты могут ранжироваться с помощью присваиваемых им весов $w_1, \dots, w_j, \dots, w_n$. Значения весов могут, в частности, отражать успешность (либо неудачи) того или иного эксперта в предшествующих прогностических процедурах. Таким образом на базе рассматриваемой схемы может быть организована некоторая постоянно функционирующая система сценарного прогнозирования.

«Традиционным» направлением для критики сценарных методов является субъективизм, неизбежно присущий любым экспертным системам. Эта проблема отчасти может быть преодолена при комплексном применении сценарных и теоретико-игровых методов. Структурная («древообразная») идентичность моделей позволяет экстраполировать выводы, получаемые относительно равновесных траекторий в динамических байесовых играх на соответствующие сценарные схемы.

VI. Результаты и обсуждение

Как уже отмечалось выше, настоящее исследование относится к серии работ, рассматривающих возможности применения теоретико-игровых методов к проблематике управления безопасностью и устойчивостью информационных систем. Его принципиальное отличие от предшествующих работ заключается в переходе от матричных к биматричным (неантагонистическим играм) при моделировании ситуации конфликта между стороной, защищающей информационную систему, и стороной, предпринимающей атаки на неё.

Подобный подход позволяет подняться на более высокий уровень обобщения и, в частности, учесть случаи, в которых проигрыш одной из сторон является зеркальным отражением выигрыша другой. Дополнительным доводов в пользу биматричных моделей является и то соображение, что эффекты защищающегося и атакующего в случае инфосистем имеют разную природу и их трудно измерить в сопоставимых единицах. Тем более, привести к одним и тем же измерителям.

Нахождение решения (равновесия в смешанных стратегиях) для биматричных моделей является ощутимо более сложной задачей, чем в случае матричных игр. Однако на численному уровне она является вполне разрешимой.

Одновременно к предложенной форме моделей могут быть успешно приложены концепции очищения равновесия, то есть правила выбора из нескольких равновесий тех, которые представляются более предпочтительными по тем или иным критериям. В настоящий работе это было продемонстрировано на

примере равновесия дрожащей руки.

В условиях современного мира, характеризующегося повышенной волатильностью и нестабильностью, особое значение приобретают задачи построения обоснованных прогнозов. Нельзя не признать, что традиционные эконометрические модели, предполагающие репликацию прошлых трендов и закономерностей, оказываются неадекватными по отношению к новым трендам и вызовам. Большей привлекательностью в этом плане обладают модели и методы сценарного прогнозирования.

Необходимо отметить содержательную близость между методами сценарного прогнозирования и динамическими играми с неполной информацией (динамическими байесовыми играми), в которые может быть трансформирована БИМВИСАС. При этом открываются широкие возможности для сравнительного анализа экспертных оценок, традиционно применяемых в сценарных прогнозов, с представлениями участников байесовой игры, моделирующей процессы защиты/атаки для информационной системы.

VII. Заключение

Радикальное повышение уровня конфликтности в экономике, обществе на международной арене резко повышают актуальность задач обеспечения безопасности и устойчивости информационных систем. Успешное решение подобных задач не может быть найдено исключительно на уровне повседневной эмпирики. Оно также требует фундаментальных научно-теоретических разработок. Стохастической природе проблем защиты информационных систем объективно соответствуют математические методы принятия решений в условиях неопределённости, в частности теории игр.

В ходе проведённых исследований была продемонстрирована перспективность и плодотворность подходов к моделированию закономерностей противостояния между защищающейся и атакующей сторонами в информационной среде. Логика равновесных по Нэшу решений позволяет выделять промежутки условной стабильности выбора методов защиты и нападения. Одновременно в случае динамической имплементации открываются конструктивные возможности оценки продолжительности интервалов стабильности и диагностирования «переломных моментов».

Развитие игровых подходов предполагает расширение класса игр, привлекаемых к моделированию проблем информационной безопасности. В частности, эволюционных игровых моделей, а также методов современной теории кооперативных игр.

Библиография

[1] Бурькова Е.В., Вавилина Т.С. Формализованная модель метода выбора стратегии противодействия нарушителям информационной безопасности на основе теории игр // Фундаментальные и прикладные исследования в современном мире. 2019. № 26-2. С. 10-15.

[2] Зима О.И. Цифровой юань: новые возможности и последствия // «Менеджмент XXI века: экономика, общество и образование в условиях новой нормальности»: сборник научных статей по материалам XX международной научно-практической онлайн конференции, Санкт-Петербург, 24–25 ноября 2021 года / под ред. А. О. Кравцова, М.В. Жаровой. Санкт-Петербург: Изд-во РГПУ им. А. И. Герцена, 2022.

[3] Зима О.И. Возможные подходы к построению инновационной модели банка, готовность к внедрению цифрового рубля // В сборнике: Государство и бизнес. Современные тенденции и проблемы развития экономики. Материалы XIII Международной научно-практической конференции. В 3-х частях. Санкт-Петербург, 2021. С. 263-271.

[4] Клименко И.С. Математическая модель комплексной защиты инфокоммуникационного объекта на основе «Игры с Природой» // Современная наука и инновации. 2022. №1 (27). С. 34–43.

[5] Конюховский П.В. Проблемы прогнозирования процессов эволюции цифровых валютных инструментов // Экономика Северо-Запада: проблемы и перспективы развития. 2022. № 3 (70). С. 55-66.

[6] Конюховский П.В., Зима О.И. Роль валютных инструментов в трансформации современной экономики // Финансы и бизнес. 2022. Т. 18. № 3. С. 3-23.

[7] Кунаковская О.В., Меньших Т.В. Применение методов теории игр к задачам информационной безопасности // Некоторые вопросы анализа, алгебры, геометрии и математического образования. 2016. № 5-1. С. 173-174.

[8] Панфилов Г.О., Чугунов А.В., Кабанов Ю.А. Электронное участие в российских регионах: результаты мониторинга 2020–2022 гг. // Государство и граждане в электронной среде. Выпуск 6 (Труды XXV Международной объединенной научной конференции «Интернет и современное общество», IMS-2022. Санкт-Петербург, 23–24 июня 2022 г. Сборник научных статей. 2022.

[9] Ремесник Е.С. Применение теории игр к оценке рисков информационной безопасности предприятия // Проблемы информационной безопасности / Труды V Всероссийской с международным участием научно-практической конференции, Симферополь-Гурзуф, 14-16 февраля 2019. С.161-163.

[10] Руденко Л.И., Пушкарева Е.В. Моделирование оценки рисков информационной безопасности // Сборник трудов конференции «Проблемы информационной безопасности». V Всероссийская с международным участием научно-практическая конференция. Крымский федеральный университет имени В.И. Вернадского. 2019. С. 163-165.

[11] Хованов Н.В. Анализ и синтез показателей при информационном дефиците. СПб., СПбГУ, 1996.

[12] Хованов Н.В. АСПИД – система квалиметрических методов оценивания в условиях дефицита информации качества сложных технических объектов // Методология и практика оценивания качества продукции. Л., ЛДНТП, 1988. С. 56-61.

[13] Хованов Н.В. Математические модели риска и неопределенности. СПб., СПбГУ, 1998.

[14] Khoury J., Nassar M. A hybrid game theory and reinforcement learning approach for cyber-physical systems security // NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium. IEEE. 2020. С. 1-9.

[15] Liu L., Huang C., Fang Y., Wang Z. Network attack and defense game theory based on Bayes-Nash equilibrium. KSII Transactions on Internet and Information Systems (TIIS). 2019. № 13(10). С. 5260-5275.

[16] Selten R. Spieltheoretische Behandlung eines Oligopolmodells mit Nachgetragheit // Zeitschrift fur die Gesamte Staatswissenschaft, 1965. № 121. С. 301–324.

П.В. Конюховский закончил Ленинградский государственный университет в 1987 г. по специальности «экономическая кибернетика». Имеет опыт в разработке автоматизированных программных систем на основе СУБД разных поколений. Длительное время работал на кафедре экономической кибернетики экономического факультета СПбГУ.

В настоящее время – профессор кафедры отраслевой экономики и финансов Института экономики и управления Российского государственного педагогического университета им.А.И. Герцена, профессор кафедры бизнес-информатики (Северо-Западный институт управления, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации).

Основные научные интересы в настоящее время связаны с моделями и методами принятия решений в условиях неопределённости, применением моделей и методов теории игр в анализе процессов

цифровой трансформации экономики и общества, методам анализа сферы образования.

А.А. Шабалин закончил Санкт-Петербургский Горный университет, бакалавр по направлению «Разработка нефтегазовых месторождений» (2019 г.), магистр по направлению «Проектное управление в нефтегазовой отрасли» (2021 г.). В настоящее время является аспирантом кафедры бизнес-информатики факультета экономики и финансов СЗИУ РАНХиГС по направлению «Системный анализ, управление и обработка информации». Профессиональная деятельность связана со сферой информационной безопасности, аналитик информационной безопасности «ЭнДжиАр Софтлаб» (Angara Technologies Group, Москва). Сфера научных интересов – защита информационных систем, теория игр, управление рисками.

Game-theoretic Approaches in The Analysis of Corporate Information Systems Protection Strategies

Pavel V. Konyukhovskiy, Andrey A. Shabalin

Abstract— **The paper is devoted to the problems of applying models and methods of strategic game theory to describe the processes of functioning of information systems. A bimatrix game model of information system interaction with an aggressive external environment is proposed. In this game the possible strategies of information system protection are formalized to a set of actions: priority of hardware, priority of third-party software, priority of own software, reliance on external expertise, reliance on a rigid security regime. Targeted sustained attack, random search, insider attack, hacking of adjacent system are considered as possible strategies of the attacking party. Under the assumption that it is possible to build a system of utility of the game on the basis of expert assessments, was demonstrated the possibilities of its analysis using the concept of Nash equilibrium, as well as its special case – «the trembling hand equilibrium».**

Separately, the paper considers possible ways of transformation of the basic static bimatrix model into a repeating game, as well as into a dynamic game with incomplete information. The latter direction is of particular interest, as it is more adequate to the realities of information protection and maintenance of sustainable functioning of information systems. In particular, the possibility of applying the concept of perfect Bayes-Nash equilibrium to develop a systematic protection policy has been demonstrated. A promising direction of implementation of the proposed models is their complex use together with systems (algorithms) of scenario forecasting.

Keywords— **Information System, Security, Stability, Game-theoretic Models of Information Systems Security, Bimatrix games, Dynamical Bayesian Games.**

REFERENCES

[17] Burkova E.V., Vavilina T.S. Formalizovannaya model' metoda vybora strategii protivodejst-viya narushitelyam informacionnoj bezopasnosti na osnove teorii igr [Formalized model of the method for selecting a strategy for countering information security intruders based on game theory] // Fundamental'nye i prikladnye issledovaniya v sovremennom mire [Fundamental and Applied Research in the Modern World]. 2019. No. 26–2. P. 10-15.

[18] Zima O.I. Cifrovoj yuan: novye vozmozhnosti i posledstviya [Digital Yuan: New Opportunities and Impact] // «Menedzhment XXI veka: ekonomika, obshestvo i obrazovanie v usloviyah novoj normalnosti»: sbornik nauchnyh statej po materialam XX mezhdunarodnoj nauchno-prakticheskoj onlajn konferencii [«Management of XXI century: economy, society and education in the conditions of new normality»: collection of scientific articles on the materials of XX international scientific-practical online conference], Sankt-Peterburg, 24–25 noyabrya 2021 goda / pod red. A.O.Kravcova,M.V.Zharovoj. Sankt-Peterburg : Izd-vo RGPU im. A.I.Gercena, 2022.

[19] Zima O.I. Vozmozhnye podhody k postroeniyu innovacionnoj modeli banka, gotovnost k vnedreniyu cifrovogo rublya [Possible Approaches to Building an Innovative Bank Model, Readiness for the Implementation of the Digital Ruble] // V sbornike: Gosudarstvo i biznes. Sovremennye tendencii i problemy razvitiya ekonomiki. Materialy XIII Mezhdunarodnoj nauchno-prakticheskoj konferencii [State and Business. Modern trends and problems of economic development. Materials of XIII International Scientific and Practical Conference]. V 3-h chastyah. Sankt-Peterburg, 2021. P. 263-271.

[20] Klimenko I.S. Matematicheskaya model' kompleksnoj zashchity infokommunikacionnogo ob"ekta na osnove «Igry s Prirodoj» [Mathematical model of complex protection of info-communication object on the basis of Game with Nature] // Sovremennaya nauka i innovacii [Modern science and innovation]. 2022. No. 1 (27). P. 34–43.

[21] Konyukhovskij P.V. Problemy prognozirovaniya processov evolyucii cifrovyh valyutnyh instrumentov [Problems of Forecasting the Evolution of Digital Currency Instruments] // Ekonomika Severo-Zapada: problemy i perspektivy razvitiya [Economy of the North-West: Problems and Prospects of Development]. 2022. No. 3 (70). P. 55-66.

[22] Konyukhovskij P.V., Zima O.I. Rol valyutnyh instrumentov v transformacii sovremennoj ekonomiki [The Role of Currency Instruments in the Transformation of the Modern Economy] // Finansy i biznes [Finance and Business]. 2022. Vol. 18. № 3. P. 3-23.

[23] Kunakovskaya O.V., Men'shih T.V. Primenenie metodov teorii igr k zadacham infor-macionnoj bezopasnosti [Application of Game Theory Methods to Information Security Problems] // Nekotorye voprosy analiza, algebry, geometrii i matematich-eskogo obrazovaniya. [Some Issues in Analysis, Algebra, Geometry and Mathematics Education]. 2016. No. 5-1. P. 173-174.

[24] Panfilov G.O., Chugunov A.V., Kabanov Yu.A. E-Participation in Russian Regions: Monitoring Results 2020-2022 // The State and Citizens in the Electronic Environment. Vol. 6 (Proceedings of the XXV International Joint Scientific Conference «Internet and Modern Society», IMS-2022, St. Petersburg, June 23-24, 2022). 2022.

[25] Remesnik E.S. Primenenie teorii igr k ocenke riskov informacionnoj bezopasnosti predpriyatiya [Application of Game Theory to Information Security Risk Assessment of the Firm] // Problemy informacionnoj bezopasnosti / Trudy V Vserossijskoj s mezhdunarodnym uchastiem nauchno-prakticheskoj konferencii, Simferopol'-Gurzuf [Problems of Information Security / Proceedings of the V All-Russian with International Participation Scientific-practical Conference, Simferopol-Gurzuf], 14–16 Feb 2019. P.161-163.

[26] Rudenko L.I., Pushkareva E.V. Modelirovanie ocenki riskov informacionnoj bezopasnocti // Sbornik trudov konferencii «Problemy informacionnoj bezopasnosti». V Vserossijskaya s mezhdunarodnym uchastiem nauchno-prakticheskaya konferenciya. Krymskij federal'nyj universitet imeni V.I. Vernadskogo [Modeling of information security risk assessment // Proceedings of the conference «Problems of information security». V All-Russian Scientific and Practical Conference with International Participation. V.I. Vernadsky Crimean Federal University]. 2019. P. 163-165.

[27] Hovanov N.V. Analiz i sintez pokazatelej pri informacionnom deficite [Analysis and Synthesis of Indicators Under Information Deficit]. SPb., SPbGU, 1996.

[28] Hovanov N.V. ASPID – sistema kvalimetricheskih metodov ocenivaniya v usloviyah deficita informacii kachestva slozhnyh tehnicheskih obektov // Metodologiya i praktika ocenivaniya kachestva produkcii [ASPID – system of qualimetric methods of assessment under conditions of information deficit of quality of complex technical objects // Methodology and Practice of Product Quality Assessment]. L., LDNTP, 1988. P. 56-61.

[29] Hovanov N.V. Matematicheskie modeli riska i neopredelennosti [Mathematical Models of Risk and Uncertainty]. SPb., SPbGU, 1998.

[30] Khoury J., Nassar M. A hybrid game theory and reinforcement learning approach for cyber-physical systems security. In NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium. IEEE. 2020. P. 1-9.

[31] Liu L., Huang C., Fang Y., Wang Z. Network attack and defense game theory based on Bayes-Nash equilibrium. KSII Transactions on Internet and Information Systems (TIIS). 2019. No. 13(10). P. 5260-5275.

[32] Selten R. Spieltheoretische Behandlung eines Oligopolmodells mit Nachgetragheit // Zeitschrift fur die Gesamte Staatswissenschaft, 1965. No. 121. P. 301–324.

Pavel V. Konyukhovskiy, Doctor of Economics, Professor, Department of Industrial Economics and Finance Herzen State Pedagogical University (Saint Petersburg, Russia), Russian Presidential Academy of National Economy and Public Administration, North-West Institute of Management, Professor of the Department of Business Informatics, E-mail: kon_pv@mail.ru, ResearcherID K-2981-2015, ORCID ID 0000-0002-2940-1049.

Andrey A. Shabalin, Russian Presidential Academy of National Economy and Public Administration, North-West Institute of Management, Postgraduate student of the Department of Business Informatics, Information Security Analyst at NGR Softlab, E-mail: ashabalin750@gmail.com, ORCID ID 0000-0002-9994-9421.