www.volsu.ru

ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

DOI: https://doi.org/10.15688/jvolsu10.2017.1.1

УДК 681.518:339.13
ББК 65.200

ИССЛЕДОВАНИЕ ПОДХОДОВ К МНОГОАГЕНТНОМУ МОДЕЛИРОВАНИЮ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Сергей Александрович Македонский

Кандидат технических наук,
главный специалист по информационной безопасности службы безопасности,
Волгоградский филиал АБ «РОССИЯ»
s-makedonskiy@yandex.ru
ул. Калинина, 13, 400001 г. Волгоград, Российская Федерация

Арина Валерьевна Никишова

Кандидат технических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
arinanv@mail.ru, infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Применение многоагентных систем для построения систем защиты информации обусловлено структурой современных информационных систем. Однако встает вопрос о взаимодействии агентов между собой и принятии ими решения о состоянии защищенности информационной системы в целом. Низкая скорость или точность принятия подобного решения может сделать неэффективным применение многоагентных систем защиты информации. В статье исследованы методы принятия агентами общего решения и сделан вывод о необходимости применения их комбинации для уменьшения вероятности выбора неоптимальной стратегии.

Ключевые слова: многоагентная система, агент, стратегия, принятие решений, голосование.

В связи с быстрым развитием информационных технологий защита информации подразумевает под собой контроль множества компонентов защищаемых систем, однако существующие системы не могут в полной мере обеспечить данный контроль из-за того, что имеют централизованную структуру, характеризуются неразвитыми адаптационными возможностями, пассивными механизмами обнаружения атак, значительной деградацией трафика целевых информационных потоков из-за большого объема ресурсов, выделяемых на защиту [6; 8].

Перспективным подходом к построению комплексных систем защиты информации является использование интеллектуальных многоагентных систем [4].

В отличие от классического способа, когда проводится поиск некоторого четко определенного (детерминированного) алгоритма, позволяющего найти наилучшее решение проблемы, в мультиагентных технологиях решение получается в результате взаимодействия множества самостоятельных целенаправленных программных модулей, так называемых интеллектуальных агентов [1; 5; 7].

Агент – это программно или аппаратно реализованная система, обладающая следующими свойствами:

– автономность – способность функционировать без прямого вмешательства людей или компьютерных средств и при этом осуществлять самоконтроль над своими действиями и внутренними состояниями;

– общественное поведение, то есть способность взаимодействия с другими агентами (а возможно, людьми), обмениваясь сообщениями с помощью языков коммуникации;

– реактивность – способность воспринимать состояние среды (физического мира, пользователя) через пользовательский интерфейс, совокупности других агентов, сети Internet или сразу всех этих компонентов внешней среды;

– целенаправленная активность – способность агентов не просто реагировать на стимулы, поступающие из среды, но и осуществлять целенаправленное поведение, проявляя инициативу.

В процессе функционирования многоагентной системы защиты должны решаться следующие задачи:

– взаимодействие агентов – установление динамических отношений между агентами;

– организация агентов – механизм разрешения или запрещения взаимодействий между агентами;

– принятие агентами общего решения.

Для систем защиты информации механизм принятия решений является одним из наиболее критичных, так как непринятие своевременных мер может привести к нарушению защищенности отдельного узла или всей информационной системы в целом [2; 3].

В общем виде проблема принятия решений группой агентов определяется следующим образом:

Пусть $A = \{a\}$ – множество агентов. Общее для всех них множество стратегий $X^A = \{x : A \to X\}$ (множество отображений A) – множество стратегий многоагентной системы A, состоящей из агентов $a \in A$.

Пусть для $k \in X$ и $a \in A$ определено $ж^k : a \to k$ – постоянные отображения A в X, принимающие для всех $a \in A$ одно и то же значение $k \in X$. Их подмножество $\Delta = \{(ж^k)_{k \in x}\} \subset X^A$ образует диагональ X^A.

Таким образом, проблема принятия решений формулируется следующим образом: систему, находящуюся в некотором состоянии $o \in X^A$, привести в некоторое состояние $o^k \in \Delta$, то есть агентов, находящихся в различных состояниях, привести в одно и то же состояние $k \in X$.

Основными тремя подходами к принятию решения множеством агентов являются:

– некооперативные игры;

– кооперативные игры;

– социальный выбор.

В некооперативных играх каждый агент осуществляет выбор действия x_i, принадлежащего допустимому множеству $X_i, i \in N = \{1,2,...,n\}$ – множеству агентов. Выбор агентами действий осуществляется однократно, одновременно и независимо.

Выигрыш i-го агента зависит от его собственного действия $x_i \in X_i$ и от вектора действий

$$x_{\downarrow}(-i) = (x_{\downarrow}(1), x_{\downarrow}(2), \ldots x_{\downarrow}(i-1), x_{\downarrow}(i+1), \ldots, x_{\downarrow}(n)) \in$$
$$X_{\downarrow}(-i) = \Pi_{\downarrow}(j \in N \setminus \{i\}) = X_{\downarrow} j.$$

оппонентов $N/\{i\}$, и от состояния среды $и \in \Omega$, и описывается действительно-значной функцией выигрыша $f_1 = f_1(и, x)$, где $x = (x_i, x_{-i}) = (x_1, x_2, ..., x_n) \in X = \Pi_{j \in N} X_j$.

Для принятия решений этими агентами составляется таблица, называемая платежной матрицей. Каждая измерение матрицы – это игрок, первое измерение определяет стратегии первого игрока, а второе – второго и т. д. На пересечении стратегий определены выигрыши, которые получат игроки.

В силу гипотезы рационального поведения каждый агент будет стремиться выбрать наилучшие для него действия при заданной обстановке. Обстановкой для него будет совокупность состояния среды $и \in \Omega$ и обстановки игры

$$x_{\downarrow}(-i) = (x_{\downarrow}(1), x_{\downarrow}(2), ... x_{\downarrow}(i-1), x_{\downarrow}(i+1), ..., x_{\downarrow}(n)) \in$$
$$X_{\downarrow}(-i) = \Pi_{\downarrow}(j \in N/\{i\}) = X_{\downarrow} j.$$

Следовательно, принцип принятия им решения о выбираемом действии можно записать следующим образом:

$$k_i(x_{-i}) = \max_{x_i \in X_i} f_i(и, x_i, x_{-i}), i \in N.$$

Это значит, что стратегия x для игрока a строго доминирует над стратегией x', если результат стратегии x лучше для игрока a, чем результат стратегии x', при любом выборе стратегий другими игроками, то есть стратегия, принимаемая агентом, – стратегия, которая максимизирует прибыль данного агента при любых действиях оставшихся агентов. Для того чтобы адекватно принимать решения, необходимо, чтобы каждый агент знал всю информацию о других агентах: обозреваемое состояние среды, если обозревание частичное, механизм принятия решений и возможные варианты решений.

В данной стратегии возможен случай, когда реализация доминантных стратегий агентов приносит прибыль каждому агенту или их группе намного меньше, чем при реализации недоминантных стратегий («дилемма заключенного»). Этот недостаток можно устранить путем добавления возможности общения между агентами, и такая игра называется кооперативной.

Кооперативная игра задается множеством игроков $N = \{1, ..., n\}$ и характеристической функцией $v: 2^N \to R$, ставящей в соответствие каждой коалиции игроков $S \subseteq N$ ее выигрыш.

Дележом игры (N, v) называется вектор $x = (x_1, ..., x_n)$, для которого выполняется свойство эффективности (свойство индивидуальной рациональности) $x_i \geq v(\{i\}), i \in N$.

Решением кооперативной игры обычно считается множество дележей, которые реализуемы при рациональном поведении игроков. Различные концепции решения кооперативных игр отличаются предположениями о рациональном поведении игроков.

Говорят, что дележ x доминирует над дележом по коалиции $S(x \phi_s y)$, если $\forall i \in S x_i > y_i, \sum_{i \in S} x_i \leq v(S)$. Если существует такая коалиция S, что $x \phi_S y$, говорят, что дележ x доминирует над дележом y.

Данная игра отличается от некооперативной возможностью передавать и запрашивать данные о действиях других агентов, что позволяет точно определить доминантную стратегию, реализуемую каждым агентом.

Принятие решений на основе социального выбора заключается в том, что каждый агент взаимодействия отмечает приоритетный для него набор стратегий в некотором наборе предпочтений L. Этот набор представляется для некоторого агента $a_i \in A$ в виде последовательности элементов $a_i : x_1 > x_2 > x_3$.

Таким образом, для данного агента a_i стратегия x_1 предпочтительнее стратегии x_2 и x_3, а стратегия x_2 предпочтительнее x_3.

Множество агентов, которые предпочитают стратегию x_i стратегии x_j, обозначается как $\#(x_{\downarrow} i \phi x_{\downarrow} j)$.

Наиболее предпочтительная стратегия $x \in X$ является выигрышной по условию Кондорсе. Стратегия удовлетворяет условию Кондорсе, если $\forall x' \in X, \#(x \phi x') \geq \#(x' \phi x)$. Данное условие выбирает стратегию x, определенную большинством агентов.

Однако для некоторых наборов предпочтений L не существует победителя по условию Кондорсе. Таким образом, последнее не всегда указывает конкретный вариант выбора.

Альтернативой может являться условие, основанное на идее условия Кондорсе, такое как набор Смита. Набор Смита – наименьший набор $S \subseteq X$, имеющий свойство $\forall x' \in S, \#(x \phi x') \geq \#(x' \phi x)$.

Основной класс голосований – неранжированные голосования. В данных голосованиях каждый агент отдает свой голос за одну стратегию. Примером является голосование множества.

Голосование множества. Здесь каждый агент $a \in A$ отдает свой единственный голос за стратегию. Стратегия, получившая большинство голосов, побеждает в голосовании.

Однако данный класс голосований обладает весьма ограниченной способностью выражения предпочтений агентов. Класс голосований, который устраняет данный недостаток, называется ранжированным голосованием.

Самым известным ранжированным голосованием является множество с устранением.

Множество с устранением. Каждый агент $a \in A$ имеет один голос и отдает его за наиболее предпочтительную стратегию. Стратегия с наименьшим количеством голосов удаляется из голосования, а агенты, которые за нее голосовали, голосуют заново за одну из оставшихся стратегий. Этот процесс повторяется, пока не останется одна стратегия, которая и считается победителем.

Голосование Борда. Каждый агент $a \in A$ предоставляет полный набор предпочтений L. На основании этого набора каждой стратегии начисляются очки.

Так, если существует набор предпочтений L из n стратегий, то самой предпочтительной из них начисляется $n - 1$ очко, второй – $n - 2$ очка и т. д. Последнему предпочтению не начисляется очков вообще. Победителем считается стратегия, набравшая в сумме наибольшее число очков от всех агентов.

Голосование Ненсона. Метод Ненсона – разновидность голосования Борда, который устраняет из голосования стратегии с наименьшим числом очков, повторяет голосование и опять устраняет слабые стратегии. Данная последовательность будет продолжаться до тех пор, пока не останется одна стратегия, которая будет считаться победителем.

Особенность метода Ненсона заключается в том, что он всегда возвращает стратегию из множества победителей Кондорсе, если оно не пусто, иначе возвращается стратегия из множества Смита.

Сравнение характеристик рассмотренных подходов к принятию решений приведено в таблице.

Таким образом, наилучшим подходом к принятию решений является социальный выбор. Каждый из представленных выше методов социального выбора может неадекватно выбирать стратегию из-за особенностей алгоритма выбора.

Для оценки выделенных методов социального выбора была разработана программа, на которой были проведены экспериментальные исследования.

Эксперимент 1. Пусть имеется многоагентная система, состоящая из 1 000 агентов. Предпочтения агентов имеют следующий вид:

– 499 агентов выбрали предпочтения $a > b > c$;

– 3 агента выбрали предпочтения $b > c > a$;

– 498 агентов выбрали предпочтения $c > b > a$.

В данном случае оптимальной стратегией является стратегия b, несмотря на то что ее как высокоприоритетную выбрало наименьшее число агентов. Причина этого в том, что стратегии a и c выбрали в качестве неблагоприятных 498 и 499 агентов соответственно.

Метод голосования множества должен присвоить стратегиям a, b, c баллы 499, 3, 498 соответственно и выбрать стратегию a.

Метод голосования множества с устранением на первом этапе присваивает страте-

Сравнение протоколов

Показатель	Некооперативные игры	Кооперативные игры	Социальный выбор
Принятие решений	Каждым агентом отдельно	Каждым агентом отдельно	Выбор общей стратегии, устраивающей большинство
Жесткий контроль действий агентов	Отсутствует	Отсутствует	Присутствует
Использование данных о выборе агентов для обучения	Отсутствует	Отсутствует	Присутствует

гиям *a*, *b*, *c* баллы 499, 3, 498 соответственно и удаляет стратегию *b* из набора. На втором этапе стратегиям *a* и *c* присваиваются баллы 499 и 501 соответственно и устраняется стратегия *a*. Остается только стратегия *c*.

Метод Борда должен присвоить стратегиям *a*, *b*, *c* баллы 998, 1003, 999 соответственно и выбрать стратегию *b*.

Метод Ненсона на первом этапе присваивает стратегиям *a*, *b*, *c* баллы 998, 1003, 999 соответственно и удаляет стратегию *a* из набора. На втором этапе стратегиям *b*, *c* присваиваются баллы 502, 498 соответственно и устраняется стратегия *c*. Остается только стратегия *b*.

Метод попарного удаления на первом этапе присваивает стратегиям *a*, *b*, *c* баллы 998, 1003, 999 соответственно и удаляет стратегию *a* из набора. На втором этапе стратегиям *b, c* присваиваются баллы 502, 498 соответственно и устраняется стратегия *c*. Остается только стратегия *b*.

В результате должна быть выбрана стратегия *b*, которая и была выбрана в результате работы программы (см. рис. 1).

Эксперимент 2. Пусть имеется многоагентная система, состоящая из 7 агентов. Предпочтения агентов имеют следующий вид:

– 3 агента выбрали предпочтения $a > b > c$;

– 2 агента выбрали предпочтения $b > c > a$;

– 1 агент выбрал предпочтения $b > a > c$;

– 1 агент выбрал предпочтения $c > a > b$.

В данном случае оптимальной стратегией является стратегия *a*, которая выбрана в качестве приоритетной для наибольшей группы агентов – 3 агентов, а также является второй по приоритетности еще для двух групп по одному агенту.

Метод голосования множества должен присвоить стратегиям *a*, *b*, *c* баллы 3, 3, 1 соответственно и выбрать стратегии *a* и *b*.

Метод голосования множества с устранением на первом этапе присваивает стратегиям *a*, *b*, *c* баллы 3, 3, 1 соответственно и удаляет стратегию *c* из набора. На втором этапе стратегиям *a* и *b* присваиваются баллы 4 и 3 соответственно и устраняется стратегия *b*. Остается только стратегия *c*.

Метод Борда должен присвоить стратегиям *a*, *b*, *c* баллы 8, 9, 4 соответственно и выбрать стратегию *b*.

Метод Ненсона на первом этапе присваивает стратегиям *a*, *b*, *c* баллы 8, 9, 4 соответственно и удаляет стратегию *c* из набора. На втором этапе стратегиям *a*, *b* присваиваются баллы 4 и 3 соответственно и устраняется стратегия *b*. Остается только стратегия *a*.

Метод попарного удаления на первом этапе присваивает стратегиям *a*, *b*, *c* баллы 8, 9, 4 соответственно и удаляет стратегию *c* из набора. На втором этапе стратегиям *a*, *b* присваиваются баллы 4 и 3 соответственно и устраняется стратегия *b*. Остается только стратегия *a*.

В результате должна быть выбрана стратегия *a*, которая и была выбрана в результате работы программы (см. рис. 2).

На основе результатов проведенных экспериментов можно сделать вывод о том, что в каждом методе принятия решений есть возможность выбора неоптимальных стратегий (существуют ситуации, когда выбор метода не является оптимальной стратегией).

Вариантом решения этой проблемы является использование нескольких методов

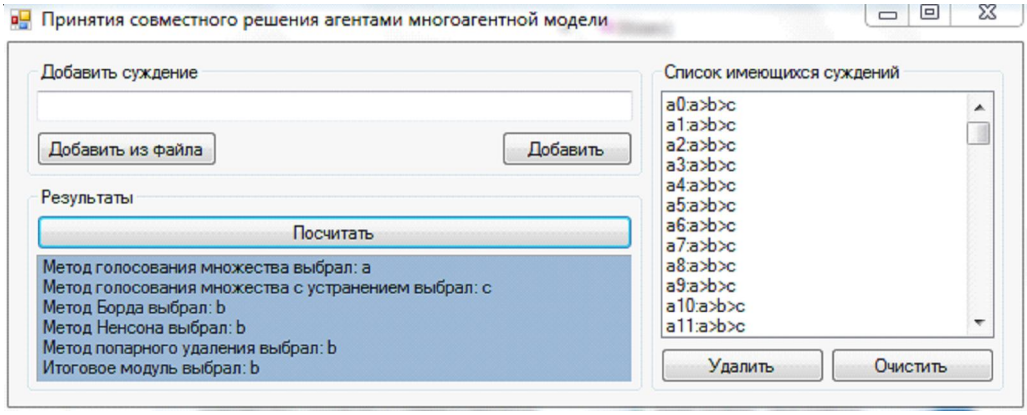

Рис. 1. Результаты эксперимента 1 (экранная копия)

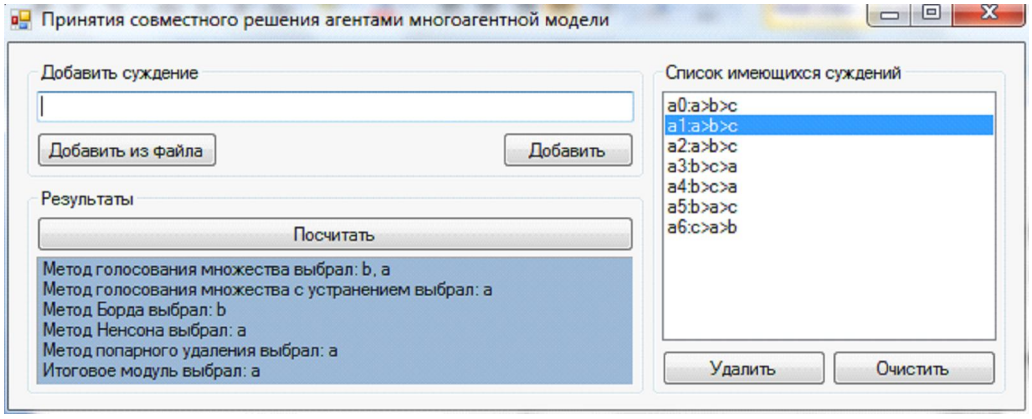

Рис. 2. Результаты эксперимента 2 (экранная копия)

принятия решений одновременно, что сводит к минимуму вероятность выбора неоптимальных стратегий.

СПИСОК ЛИТЕРАТУРЫ

1. Боровиков, В. П. Нейронные сети. STATISTICA Neural Networks: Методология и технологии современного анализа данных / В. П. Боровиков. – 2-е изд., перераб. и доп. – М. : Горячая линия Телеком, 2008. – 392 с.

2. Витенбург, Е. А. Системы поддержки принятия решений в информационной безопасности / Е. А. Витенбург, А. В. Никишова, А. Е. Чурилина // Вестник компьютерных и информационных технологий. – 2015. – № 4. – С. 50–56.

3. Кравченко, Т. К. Принятие групповых решений с использованием экспертной системы поддержки принятия решений / Т. К. Кравченко // Информационные технологии в проектировании и производстве. – 2015. – № 2. – С. 68–75.

4. Матвейкин, В. Г. Информационные системы интеллектуального анализа / В. Г. Матвейкин, Б. С. Дмитриевский, Н. Р. Ляпин. – М. : Машиностроение, 2008. – 92 с.

5. Никулин, А. Н. Аналитическая платформа «Дедуктор» – применение в информационных системах экономики / А. Н. Никулин, И. В. Черныш ев. – Ульяновск : УлГТУ, 2012. – 37 с.

6. Оладько, В. С. Модель оценки защищенности автоматизированного рабочего места пользователя / В. С. Оладько // Информационные системы и технологии. – 2016. – № 1 (93). – С. 92–99.

7. Потемкин, В. Г. Нейронные сети. MATLAB 6 / В. Г. Потемкин, В. С. Медведев. – М. : Диалог-МИФИ, 2002. – 496 с.

8. Трофимова, Л. А. Управление знаниями / Л. А. Трофимова, В. В. Трофимов. – СПб. : Изд-во СПбГУЭФ, 2012. – 77 с.

REFERENCES

1. Borovikov V.P. *Neyronnye seti. STATISTICA Neural Networks: Metodologiya i tekhnologii sovremennogo analiza dannykh* [Neural Network. STATISTICA Neural Networks: Methodology and Technologies of Modern Data Analysis]. 2nd ed., rev. and add. Moscow, Goryachaya liniya Telekom Publ., 2008. 392 p.

2. Vitenburg E.A., Nikishova A.V., Churilina A.E. Sistemy podderzhki prinyatiya resheniy v informatsionnoy bezopasnosti [System of Decision-Making Support in Information Security]. *Vestnik kompyuternykh i informatsionnykh tekhnologiy*, 2015, no. 4, pp. 50-56.

3. Kravchenko T.K. Prinyatie gruppovykh resheniy s ispolzovaniem ekspertnoy sistemy podderzhki prinyatiya resheniy [The Group Decision-Making Using Expert Systems to Support Decision-Making]. *Informatsionnye tekhnologii v proektirovanii i proizvodstve*, 2015, no. 2, pp. 68-75.

4. Matveykin V.G., Dmitrievskiy B.S., Lyapin N.R. *Informatsionnye sistemy intellektualnogo analiza* [Information Systems of Data Mining]. Moscow, Mashinostroenie Publ., 2008. 92 p.

5. Nikulin A.N., Chernyshev I.V. *Analiticheskaya platforma «Deduktor» – primenenie v informatsionnykh sistemakh ekonomiki* [The Analytical Platform "Deductor" – Application in Information Systems of the Economy]. Ulyanovsk, izd-vo UlGTU, 2012. 37 p.

6. Oladko V.S. Model otsenki zashchishchennosti avtomatizirovannogo rabochego mesta polzovatelya [Model of Evaluation of the Security of User's Workstation]. *Informatsionnye sistemy i tekhnologii*, 2016, no. 1 (93), pp. 92-99.

7. Potemkin V.G., Medvedev V.S. *Neyronnye seti. MATLAB 6* [Neural Network. MATLAB 6]. Moscow, Dialog-MIFI Publ., 2002. 496 p.

8. Trofimova L.A., Trofimov V.V. *Upravlenie znaniyami* [Knowledge Management]. Saint Petersburg, Izd-vo SPbGUEF, 2012. 77 p.

STUDY OF APPROACHES TO MULTI-AGENT MODELING OF INFORMATION PROTECTION SYSTEMS

Sergey Aleksandrovich Makedonskiy

Candidate of Technical Sciences,
Chief Specialist for Information Security of Security Service,
Volgograd Branch of AB Rossiya JSC
s-makedonskiy@yandex.ru
Kalinina St., 13, 400001 Volgograd, Russian Federation

Arina Valeryevna Nikishova

Candidate of Technical Sciences,
Associate Professor, Department of Information Security,
Volgograd State University
arinanv@mail.ru, infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. In connection with the development of information technologies, information protection means are under control of a plurality of components of the protected system. However, existing systems can not fully ensure the control due to the fact that they have a centralized structure, are characterized by poor adaptive capacity, passive mechanisms to detect attacks, a significant degradation of traffic of targeted information flows due to the large amount of resources allocated to defense. A promising approach to building complex systems of information protection is the use of intelligent multi-agent systems.

The application of multi-agent systems for building information security systems is conditioned by the structure of modern information systems. However, this arises the question about the interaction of agents among themselves and their decision-making about the state of security of the information system as a whole. Low speed or accuracy of making such decision can make the use of multi-agent systems of information protection inefficient. The article examines the methods of making the general decision by the agents. The conclusion is made on the need to use their combinations to reduce the probability of selecting a suboptimal strategy.

On the basis of experiments it can be concluded that each method of decision-making implies a non-optimal choice. Solution of this problem is the use of several methods of decision-making simultaneously, which minimizes the probability of selecting non-optimal strategies.

Key words: multi-agent system, agent, strategy, decision-making, voting.