ISSN 1814-1196
Научный вестник НГТУ
том 55, № 2, 2014, с. 105–108

http://journals.nstu.ru/vestnik
Scientific Bulletin of NSTU
Vol. 55, No. 2, 2014, pp. 105–108

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

MODERN INFORMATION TECHNOLOGIES

УДК 004.056

Формирование признаков описания агентного множества оценки информационной безопасности систем*

Ю.А. ГАТЧИН[1], С.В. ШИРЯЕВ[2]

[1] 197101, г. Санкт-Петербург, Кронверкский проспект, д. 49, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, д. т. н., зав. кафедрой, e-mail: gatchin@mail.ifmo.ru
[2] 197101, г. Санкт-Петербург, Кронверкский проспект, д.49, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, e-mail: ssv.88@inbox.ru

В работе рассматривается методика формирования признакового пространства агентного множества для решения задач структурирования агентов, моделирования и прогнозирования их поведения. Обсуждаются варианты определения дескрипторов для косвенной идентификации агентов в мультиагентной среде. Предлагаются способы конструирования моделей «агент-признак» и «агент-агент» для признаков измеренных в различных шкалах на основе репрезентативной теории измерения. Приведен возможный перечень атрибутов агентов и соответствующий ему набор интерпретаций, агрегированный по типологическому, архитектурному и организационному принципам. Для оценки информационной безопасности на основе применения агентного подхода, авторами предлагаются схемы представления сведений об агентах на основе соответствующего анализа механизмов формирования информационных шаблонов – коннекторов. В связи с отсутствием априорной математической модели анализируемых ситуаций в работе рассматривается упрощенное представление сведений об агентах. В этом случае можно использовать модель оценки с точностью до «параметров», которой соответствует реляционная модель «сущность-атрибут», ее важнейшей особенностью является замкнутость, позволяющая доказывать корректность манипулятивных операций. Показано, что на основе отображения сведений об агентном множестве в признаковом пространстве можно эффективно выполнять все последующие этапы разработки мультиагентной системы. Предлагаемая методика формирования признакового описания агентов позволяет создать новый подход к структурной организации мультиагентной среды, предназначенной для автоматизации оценки информационной безопасности систем.

Ключевые слова: интеллектуальный агент, информационная безопасность, мультиагентная среда, мониторинг нарушений, манипулятивных операций, модель «агент-признак», признаковое пространство, типология и архитектура агентов, самоорганизация агентов, реляционная модель

ВВЕДЕНИЕ

Организация мультиагентной среды, предназначенной для оценки информационной безопасности систем, связана с решением следующих проблем [1]:

– декомпозиции задачи оценки на подзадачи;

– формирования признакового пространства агентов;

– структурирования множества агентов в соответствии с делегированными им полномочиями;

– разработки механизмов взаимодействия агентов, включая координацию, кооперацию, конкуренцию и коммуникацию.

Успешность применения агентного подхода к оценке информационной безопасности [2] во многом предопределяется адекватностью представления сведений об агентах и поэтому требует тщательного и конструктивного анализа механизмов формирования агентных дискрипторов.

* *Статья получена 25 февраля 2014 г.*

ПРЕДЛАГАЕМЫЙ ПОДХОД

В области оценки информационной безопасности систем наличие мониторинга нарушений и априорных моделей оценивания скорее исключение, чем правило. Здесь на первый план выступает проблема упрощенного представления сведений об агентах [3] при отсутствии априорной математической модели изучаемого явления или ситуации. Классу моделей, допустимых при таком представлении, можно сопоставить модель оценки с точностью до «параметров», не обязательно числовых, изменения которых порождает весь рассматриваемый класс. Такой моделью естественно считать модель «агент-признак», которой соответствует известная реляционная модель «сущность-атрибут» или просто таблица. Важнейшей ее характеристикой является замкнутость. Замкнутость позволяет доказывать корректность многих манипулятивных операций. Разнообразные операторы, определенные для описания агентов, являются коммутативными, либо дистрибутивными или ассоциативными.

Модель такого рода можно анализировать в терминах агентов (сущностей, строк) или признаков (атрибутов, столбцов). Для качественного анализа язык атрибутов неудобен, поэтому здесь чаще используется язык сущностей (агентов, строк) [4]. В соответствии с репрезентативной теорией измерений свойства (признаки) могут быть измерены в различных шкалах, задаваемых множеством допустимых преобразований. Для формирования признакового описания предлагается конструировать признаки, измеренные в номинальной шкале. В этом случае следует ориентироваться на следующие два возможных способа формирования структуры «агент-признак»:

1. Номинальный признак с m-значениями характеризуется совокупностью n-мерных булевых столбцов. Столбец j содержит единицы в векторах описаний соответствующих агентов, для которых признак принимает j-е значение, а нули – в остальных описаниях (строках). Это соответствует переходу от номинального x_s к m дихотомическим признакам $x_{i,j}$ $\left(j=\overline{1,m}\right)$, сопоставляющих каждому агенту «1» («да») или «0» («нет»), в зависимости от того принимает ли x_s для данного агента j-е значение.

2. Если для реализации признакового описания дополнительная нагрузка задания одного признака несколькими столбцами оказывается критичной, то более предпочтительным является представление номинальных признаков в виде матриц «агент-агент», при котором каждому признаку отвечает единственный элемент – $n\times n$-мерного пространства. Для структурных признаков – это булевская матрица размерности $n\times n$, в которой каждый элемент фиксируется единицей, когда значение признака для агентов i и j совпадают, или нулем – в противном случае.

Подобным образом могут быть заданы и любые структурные признаки (т. е. качественные признаки с заданной структурой отношений между значениями), если j-е значение признака связано (влияет, сравнимо, и т. п.) с i-м значением, то в j-м столбце $x_{j,i}$ необходимо зафиксировать единицы в векторах – описаниях соответствующих не только j-му, но и i-му значению признаков.

Аналогично реализуется представление неоднозначных (неальтернативных) качественных признаков, а также признаков с «нечетким» определением [5].

Язык моделей «агент-агент» удобен и для задания шкал упорядочения, т. е. доминирования (рангов) и похожести (порядка). Эти шкалы удобны задавать числовым отношением «равенства с точностью до порога различимости». Иначе говоря, если A-множество агентов, а F-измеряющее отображение, то шкала похожести при пороге $\Delta_1>0$ задается отношением G по правилу

$$(a,b)\in G \leftrightarrow \left|F(a)-F(b)\right|\le \Delta_1,\ a,b\in A,$$

а шкала доминирования при пороге Δ_2 отношением H:

$$(a,b)\in H \leftrightarrow F(a)\ge F(b)+\Delta_2,\ a,b\in A.$$

Важно отметить, что рассмотренная модель конструирования признакового пространства агентов легко интегрируется в структуры хранения и, в первую очередь, в экстенсиональную (фактуальную) компоненту баз знаний [6].

Для конструирования моделей «агент-признак» можно использовать множество основных свойств агентов и их потенциально возможные интерпретации (значения):

- X_1 – среды функционирования агентов (трансформируемая замкнутая, трансформируемая открытая, нетрансформируемая замкнутая, нетрансформируемая открытая, замкнутая детерминированная, замкнутая вероятностная, вероятностная стационарная);

- X_2 – типология агентов (поддержка автономности, поддержка активности, использование базовых знаний, использование убеждений, использование намерений, обязательств и желаний, поддержка социального поведения);
- X_3 – архитектура агентов (продукционная, Холланда, Барбучеану-Фокса, с трехуровневой базой знаний, BDI, коннекционисткая, гибридная);
- X_4 – самоорганизация (координация X_4^1, кооперация X_4^2, конкуренция X_4^3, коммуникация X_4^4).

Интерпретация признака «координация» X_4^1 должна включать согласование целей, выработку оценки референтности, оценку конформности, разрешение конфликтов, формирования обязательств, выработку соглашений. Возможными значениями признака «кооперация» X_4^2 являются ее четыре основные функции: традиционная, директивная, спонтанная, контрактная. Специфика конкуренции X_4^3 проявляется на уровне правил и санкций. Наконец, «коммуникация» X_4^4 характеризуется поддержкой трех базовых функций: фактической, информационной и управленческой.

Приведенный перечень, естественно, не исчерпывает все многообразие свойств агентов и при необходимости может быть изменен или дополнен. Расширение списка признаков, претендующих на включение, можно осуществить, например, путем добавления в него инструментальных средств функционально-ролевой поддержки агентов и (или) сервисов с соответствующими стандартными протоколами.

ЗАКЛЮЧЕНИЕ

Корректное отображение сведений об агентном множестве в признаковое пространство является непременным условием правильности выполнения всех последующих этапов разработки мультиагентной системы. В первую очередь это касается этапа структурирования агентного множества [7] с целью определения однородных групп агентов с последующей оценкой их референтности и адресности делегируемых им полномочий. Реализация предложенной методики формирования признакового описания агентов должна способствовать созданию единообразного подхода к структурной организации мультиагентной среды, предназначенной для автоматизации оценки информационной безопасности системы.

СПИСОК ЛИТЕРАТУРЫ

[1] **Москаленко Ю.С.** Организация систем, основанных на знаниях: учеб. пособие. – Владивосток: Изд-во Дальневост. федер. ун-та, 2013. – 250 с.

[2] **Варлатая С.К., Москаленко Ю.С., Ширяев С.В.** Агентный подход к оценке информационной безопасности корпоративных систем // Науч. вестн. НГТУ. – 2014. – № 1 (54). – С. 66–71.

[3] **Люгер Дж.Ф.** Искусственный интеллект: стратегии и методы решения сложных проблем: пер. с англ. – 4-е изд. – М.: Вильямс, 2003. – 864 с.

[4] **Костров Б.В., Ручкин В.Н., Фулин В.А.** Основы искусственного интеллекта. – М.: ДЕСС, 2007. – 192 с.

[5] **Рассел С., Норвиг П**. Искусственный интеллект: современный подход. – 2-е изд. – М.: Вильямс, 2005. – 1408 с.

[6] **Prieto-Diaz R**. The common criteria evaluation process explanation, shortcomings, and research opportunities // Technical Report CISC-TR-2002-03, december 2002-CISC / Commonwealth Inform. Security Center. – Harrisonburg, Virginia, USA: James Madison Univ., 2002. – 56 p.

[7] **Shoham Y., Leyton-Brown K.** Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations. – Cambridge Univ. Press, 2008. – 507 p.

Гатчин Юрий Арминакович, доктор технических наук, профессор, заведующий кафедрой проектирования и безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики. Основное направление научных исследований – информационная безопасность. Имеет более 80 публикаций. E-mail: gatchin@mail.ifmo.ru

Ширяев Сергей Вячеславович, аспирант кафедры проектирования безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики. Основное направление научных исследований – информационная безопасность. Имеет 5 публикаций. E-mail: ssv.88@inbox.ru

*Formation of features for describing an agent set of system information security assessment**

Y.A. GATCHIN[1], S.V. SHIRYAEV[2]

[1] Saint-Petersburg State University of Information Technologies, 49, Kronverksky Prospekt, St. Petersburg, 197101, Russian Federation, D.Sc.(Eng.), head of department, e-mail: gatchin@mail.ifmo.ru
[2] Saint-Petersburg State University of Information Technologies, 49, Kronverksky Prospekt, St. Petersburg, 197101, Russian Federation, postgraduate student, e-mail: ssv.88@inbox.ru

The method of forming an agent set feature space for solving problems of structuring agents as well as modeling and predicting their behavior are considered in the paper. Options for determining descriptors for indirect identification of agents in a multi-agent environment are discussed. Ways of building "agent - feature " and " agent - agent" models for the characteristics measured in different scales based on a representative measurement theory are proposed. A possible list of agent attributes and a corresponding set of their interpretations aggregated according to typological, architectural and organizational principles is given. To assess information security through the use of the agent-based approach, the authors propose schemes for representing information about the agents on the basis of an appropriate analysis of the mechanisms of the information templates – connectors formation. As an a priori mathematical model of the situation to be analyzed is not available, the authors consider a simplified representation of information about agents. In this case, you can use a "parameter-accurate" assessment model which corresponds to the "entity-attribute" relational model, its most important feature being isolation, which allows proving the correctness of the manipulative operations. It is shown that using mapping information about an agent-based set in the feature space it is possible to effectively perform all subsequent stages of the multi-agent system development. The proposed method of feature descriptions of agent forming makes it possible to create a new approach to the structural organization of the multi-agent environment intended for automation of information security assessment systems.

Keywords: intelligent agent, information security, multi-agent environment, control of violations of manipulative operations, model "agent-feature, feature space, the typology and architecture of agents, self-organizing agents, the relational model

REFERENCES

[1] Moskalenko Iu.S. *Organizatsiia sistem, osnovannykh na znaniiakh* [The organization of the systems founded on knowledge]. Vladivostok, Far Eastern Federal Univ. Publ., 2013. 250 p.

[2] Varlataia S.K., Moskalenko Iu.S., Shiriaev S.V. Agentnyi podkhod k otsenke informatsionnoi bezopasnosti korporativnykh system [Agent-based method to the assessment of corporate systems information security]. *Nauchnyi vestnik NGTU* [Science Bulletin of Novosibirsk State Technical University], 2014, no. 1 (54), pp. 66-71.

[3] Liuger D.F. Artificial Intelligence: Strategies and methods for solving complex problems. Moscow, Williams Publ., 2003. 864 p.

[4] Kostrov B.V., Ruchkin V.N., Fulin V.A. *Osnovy iskusstvennogo intellekta* [Bases of artificial intelligence]. Moscow, DESS Publ., 2007. 192 p.

[5] Russel S., Norvig P. *Artificial intelligence. A modern approach*. Second ed. Prentice Hall, 2003. (Russ. ed.: Rassel S., Norvig P. *Iskusstvennyi intellekt. Sovremennyi podkhod*. 2-e izd. Moscow, Williams Publ., 2005. 1408 p.).

[6] Prieto-Diaz R. The common criteria evaluation process explanation, shortcomings, and research opportunities. Commonwealth Information Security Center Technical Report CISC-TR-2002-03, December 2002-CISC, James Madison University, USA. 56 p.

[7] Shoham Y., Leyton-Brown K. Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations. Cambridge Univ. Press, 2008. 507 p.

ISSN 1814-1196, http://journals.nstu.ru/vestnik
Scientific Bulletin of NSTU
Vol. 55, No. 2, 2014, pp. 105–108

* *Manuscript received February 25, 2014.*