УДК 621.396.41

С.К. Варлатая, Ю.С. Москаленко, С.В. Ширяев

Структурирование агентного множества оценки информационной безопасности корпоративных систем

Рассмотрены проблемы организации мультиагентной среды, предназначенной для оценки информационной безопасности системы. Предлагаются принципы формирования признакового пространства агентов и поиска их однородных функционально-ролевых групп.
Ключевые слова: агентное множество, агентный подход, мультиагентная система, типология агентов, архитектура агентов, кластерный анализ, оценка информационной безопасности.

Постановка задачи. Эффективность оценки информационной безопасности систем во многом зависит от степени автоматизации мероприятий по выработке политики безопасности и внедрению современных средств интеллектуальных информационных технологий.

Одно из перспективных направлений автоматизации оценки безопасности информационных систем связано с применением и внутренним развитием мультиагентных технологий [1]. При этом предполагается, что отдельный агент имеет лишь частичное представление об общей задаче оценки и способен решать некоторые её подзадачи в соответствии с делегированными ему функциями или ролью [2]. В рамках этой парадигмы эффективность мультиагентного подхода во многом предопределяется эффективностью взаимодействия агентов, которая неотделима от её организационной структуры. В развитие агентного подхода [3] в настоящей работе рассматриваются вопросы структурирования агентного сообщества на основе косвенной идентификации агентов и процедур кластеризации, инвариантных к топологическим особенностям агентных групп.

Предлагаемые решения. Необходимая и достаточная мощность агентного множества A определяется нормой подмножеств подзадач $|S|$, делегируемых агентам для оценки безопасности системы. Структурирование агентного сообщества осуществляется различными способами, но предпочтение всегда следует отдавать процедурам, не связанным, по крайней мере явно, с введением жестких классификационных критериев. Рассмотрим один из возможных вариантов такого принципа.

Пусть $a_j = (x_1, x_2, ..., x_n)$ – описание агента $a_j \in A$ в признаковом пространстве X. В качестве признаков будем использовать свойства агентов, измеренные в номинальной шкале. Напомним, что признак является номинальным, если множество его допустимых преобразований состоит только из взаимно однозначных преобразований. Хотя формирование признакового описания чаще всего происходит на интуитивном уровне, косвенная идентификация агентов представляется безальтернативной.

Рассматриваемое множество X предлагается определять по крайней мере четырьмя группами признаков: X_1, X_2, X_3 и X_4. Первая группа характеризует тип решаемых подзадач оценки безопасности и идентифицирует сервисы, предназначенные для их решения. При ориентации на CommonCriteria общей методологии оценки ОМО [3] эта группа должна включать в себя функциональную подгруппу (наличие аудита безопасности, наличие идентификации и аутентификации, использование ресурсов), подгруппу производных параметров (связи, приватности, защиты пользовательских данных и защиты функций безопасности объекта) и, наконец, подгруппу инфраструктурных атрибутов (криптографической поддержки, управления безопасностью, доступа к объекту, доверенного маршрута).

Вторая группа признаков X_2 отображает типы сред функционирования агентов, включая замкнутые и открытые, трансформируемые и нетрансформируемые, детерминированные, вероятностные, стационарные и нестационарные среды [4].

Третья группа X_3 характеризует типологию агентов. Обязательным является включение в эту группу следующих свойств агентов:

– поддержка автономности;

– поддержка социального поведения;

– поддержка активности;

– использование базовых знаний;

– использование убеждений;

– использование намерений, обязательств и желаний.

Четвертая группа признаков X_4 предназначена для идентификации типа архитектуры агентов: продукционной, Холланда, с трехуровневой базой знаний, BDI, коннекционистской, гибридной [4].

В общем случае глоссарий множества признаков X может быть иным.

Структурирование агентного множества A, представленного совокупностью описаний $\{a_j\}^k$, будем рассматривать как процедуру кластеризации – разбиения множества A на известное или не известное заранее число групп, с некоторыми неформальными требованиями:

– внутри групп описания агентов должны быть сильно связанными;

– между группами описания агентов должны быть слабо связными.

Под связностью понимается некоторая мера близости или расстояния. Эти требования отображают стандартную гипотезу компактности или «развала на кучи».

Нацеленность методов кластерного анализа на определенную структуру группировок агентов в пространстве признаков X может приводить к неоптимальным или даже неадекватным результатам, если гипотеза о типе группировок не верна. Традиционно в качестве критериев кластеризации используют два различных вида показателей [4]: оценочные индексы Мезиха (внешний критерий значимости, кофенетический коэффициент Сокала–Рольфа, меру воспроизводимости) и структурные характеристики кластеров (степень близости элементов внутри класса, среднюю длину ребер графа *i*-го кластера и т.п.). Это приводит, во-первых, к тому, что имеющейся совокупности данных фактов «навязывают» не присущую им структуру и тем самым искажают реальную интерпретацию группировки. Во-вторых, такой подход приводит к известным проблемам неоднозначности результатов (например к локальностям) при многопараметрической оптимизации.

Альтернативой описанной оценки решений может служить процедура, основная идея которой сводится к следующему. Пусть задано множество $A=(a_1,a_2,...,a_n)$, состоящее из *n* агентов. Система $R=(R_1,R_2,...,R_m)$ непустых множеств $R_i \in A$ называется разбиением множества A, если всякий элемент a_k содержится в одном и том же множестве $R_i\left(i=\overline{i,m}\right)$, т.е.

$$U_{i=1}^{m} R_i = A \text{ и } R_i \cap R_j = \otimes, i \neq j .$$

Множества $R_1,...,R_m$ являются классами разбиения R.

Во множестве всех разбиений на A можно определить разбиения, лежащие «между» другими. Например, если разбиение S получается из разбиения R объединением некоторых его классов, а разбиение T – аналогичным образом из S, то разбиение S лежит между R и T: [R, S, T].

С другой стороны, разбиениям R, S, T соответствуют отношения эквивалентности ρ,σ,τ. Исходя из этого, разбиение S лежит между разбиением R и T тогда и только тогда, когда

$$\rho \cap \tau \subset \sigma \subset \rho \cup \tau .$$

В терминах «между» крайними разбиениями будут: тривиальное, состоящее из одного агента, и универсальное, состоящее из всех агентов множества A. Идентификаторами отношений эквивалентности являются соответствующие им матрицы смежности [4]. Поэтому для оценки «похожести» разбиений естественно ввести расстояние между ними как некоторую индикаторную функцию, определяемую по величине разности сравниваемых матриц смежности. В этом случае вычислительная проблема упрощается вплоть до тривиальной и задача состоит в том, чтобы на множестве получаемых разбиений организовать процедуру последовательной оценки следующего разбиения по отношению к предыдущему с помощью найденного между ними расстояния. Если это расстояние ϑ сохраняет свое минимальное значение ε и

$$\vartheta = \varepsilon + \Delta ,$$

где Δ – константа, характеризующая устойчивость группировки на некотором наперед заданном интервале, то разбиения, попавшие в этот интервал, и есть исконные.

Нетрудно заметить, что предлагаемый подход инвариантен к характеру распределения агентов на множестве A и не опирается на какие-либо навязываемые извне топологические ограничения на группы агентов.

Заключение. Таким образом, в данной работе на основе современной технологии интеллектуальных агентов сформулированы и предложены решения, связанные с формированием признакового описания агентного сообщества оценки безопасности информационных систем и с явным определением его организационной структуры в теоретико-множественных терминах согласования разбиений.

Литература

1. Люгер Дж.Ф. Искусственный интеллект: стратегии и методы решения сложных проблем. – М.: Вильямс, 2005. – 864 с.

2. Рассел С. Искусственный интеллект. Современный подход / С. Рассел, П. Норвиг. – М.: Вильямс, 2005. – 1408 с.

3. Москаленко Ю.С. Агентный подход к оценке информационной безопасности корпоративных систем / Ю.С. Москаленко, С.К. Варлатая, С.В. Ширяев // Научный вестник НГТУ. – 2014. – № 1 (54). – С. 66–71.

4. Москаленко Ю.С. Организация систем, основанных на знаниях. – Владивосток: Изд. дом «Дальневосточный федеральный университет», 2013. – 242 с.

Варлатая Светлана Климентьевна
Канд. техн. наук, профессор каф. информационной безопасности школы естественных наук Дальневосточного федерального университета (ДВФУ ШЕН)
Тел.: 8-924-734-92-05
Эл. почта: sk-varl@yandex.ru

Москаленко Юрий Сергеевич
Канд. техн. наук, профессор каф. информационной безопасности ДВФУ ШЕН
Тел.: 8 (423) 224-20-74
Эл. почта: moskalenko.ys@dvfu.ru

Ширяев Сергей Вячеславович
Аспирант каф. проектирования безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Тел.: 8-921-447-71-08
Эл. почта: ssv.88@inbox.ru

Varlataya S.K., Moskalenko Y.S., Shiryaev S.V.
Structuring agent-based set of corporate information security assessment systems.

The paper discusses the problems of the organization of multi-agent environment, designed to assess information security system. Offered principles of feature space agents and search their functional role of homogeneous groups.
Keywords: agent-based set, agent-based approach, multi-agent system, the typology of agents, agents architecture, cluster analysis, evaluation of information security.