Научный вестник НГТУ. – 2014. – № 1(54)

УДК 004.056

Агентный подход к оценке информационной безопасности корпоративных систем*

С.К. ВАРЛАТАЯ[1], Ю.С. МОСКАЛЕНКО[1], С.В. ШИРЯЕВ[2]

[1] *Владивосток, Дальневосточный федеральный университет*
[2] *Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет Информационных технологий, механики и оптики*

В статье обсуждаются проблемы разработки интеллектуальных средств оценки информационной безопасности систем на основе мультиагентной технологии. Предложена общая методика оценки безопасности компьютерных систем на основе анализа политики безопасности с выбором показателей защищаемости системы, установления их значений, и сравнения с эталоном. При оценивании показана необходимость многократной оперативной коррекции используемых показателей. В работе на основе агентно-ориентированой технологии использующей интеллектуальных агентов как высокоуровневую абстракцию рассмотрены варианты формализации и структурирования проблемной области. Показано, что интеллектуальный агент должен иметь возможность взаимодействия с пользователем для получения соответствующих заданий и возврата полученных результатов. Разработанный метод, учитывая требования, основанные на унификации критериев и способов оценки информационной безопасности, позволяет оперативно корректировать принимаемые решения при изменениях в описаниях мероприятий за счет гибкости и автономности агентов, вне зависимости от методов оценивания. В качестве примера в статье рассматривается возможный вариант оценки информационной безопасности, когда критерии оценки интерпретируются как нечеткие суждения. Показана возможность оперативной коррекции показателей и критериев оценки при многократном изменении условий проведения мероприятий оценки по информационной безопасности. Рассматриваются вопросы целеполагания, организации баз знаний и планирования поведения агентов. Анализируются схемы информационного взаимодействия агентов, решение подзадач на уровне сервисов, способы обеспечения эксплицитности содержимого баз знаний и интерпретируемости хода решения подзадач.

Ключевые слова: информационная безопасность, оценка безопасности, пространство состояний, коррекция состояний, критерии, интеллектуальный агент, мультиагентная система, база знаний, сервисы, архитектура агентов, социальное поведение агентов.

ВВЕДЕНИЕ

Оценка информационной безопасности систем представляет собой комплекс мероприятий, связанных с выработанной или выбором показателей, методом определения и установление их значений, включая базовые, а также сравнение последних с эталонными. Например, обеспечение информационной безопасности с платформой систем автоматического управления промышленных предприятий связано с проведением следующих мероприятий:

- оценкой встроенных средств защиты, включая средства авторизации ОС;
- оценкой организации виртуальной частной сети *(VPN)* в канале передачи данных;
- оценкой шифрования трафика;
- оценкой использования электронной подписи;
- оценкой использования беспроводных устройстве;
- оценкой регламентации работы с защищенной системой и т. п.

Комплексная оценка безопасности требует согласования подобного рода оценок и является достаточно сложной задачей. Решение этой и зависимых от неё других проблем, как правило, связанно с унификацией и стандартизацией критериев и методик оценивания.

* *Статья получена 19 ноября 2013 г.*

Типичным примером такого подхода является общая методика оценки безопасности *ОМО* на основе *Common Criteria (CC)* [1], в которой представлены критерии для оценки безопасности программно-технического уровня. В общем случае, при оценивании возникает необходимость многократной оперативной коррекции используемых показателей и введения новых критериев и методов оценивания. Характерным требованием к средствам оценивания при этом является их способность к глубокой интерпретации результатов, включая обеспечение ответов на вопросы пользователей, оценщиков, экспертов «что будет, если…?» и «что необходимо сделать, что бы…?».

Проектирование и реализацию такого рода средств оценивания предлагается осуществлять в рамках агентно-ориентированной технологии, использующей интеллектуальных агентов как высокоуровневую абстракцию для формализации и структурирования проблемной области и как мощное средство для разработки соответствующего инструментария в виде мультиагентной системы.

Суть агентной парадигмы состоит в делегировании полномочий. Интеллектуальный агент – программно-аппаратная сущность – должен иметь возможность взаимодействия с пользователем для получения соответствующих заданий и возвращения полученных результатов, ориентироваться в среде своего выполнения и принимать решения, необходимые для выполнения поставленных перед ним задач.

Common Criteria оценивает инфраструктуру (framework), в которой разработчики могут заявить о свойствах безопасности продуктов. В соответствии с этим в общей методологии оценки *(ОМО)* описываются основные действия оценщиков и экспертов органов по спецификации при проведении оценочных мероприятий. Указанные действия могут быть делегированы агентам, а *СС* использованы для целеполагания, описания критериев, выработки планов поведения и интерпретации результатов и, наконец, определения согласованной комплексной оценки.

Предлагаемый подход с одной стороны учитывает требования, связанные с унификацией критериев и способов оценки безопасности, а с другой – позволяет оперативно корректировать принимаемые решения при изменениях в описаниях мероприятии, за счет таких свойств агентов как ситуативность, автономность, гибкость, социальность, вне зависимости от того насколько примитивные или изощренные методы оценивания применяются.

ПРЕДЛАГАЕМЫЙ ПОДХОД

Задачу Z оценки информационной безопасности систем будем рассматривать как совокупность подзадач $\{z_i\}^p$, полученных в результате декомпозиции исходной. Характер и глубина декомпозиции определяется возможностью выделения «базовых» и «производных» подзадач, а также имеющимися информационными, локальными, критическими, разделяемыми и защищенными ресурсами.

Каждую подзадачу $z_i \in Z$ представим с помощью следующего коннектора (описателя):

$$z_i = (\alpha, GOAL, H, S, SRV, M, T_1, T_2), \quad (1)$$

где α – идентификатор подзадачи; $GOAL$ – цель; H – совокупность сведений, используемых при решении z_i; S – множество методов(планов) решения подзадачи z_i; SRV – множество сервисов, которые могут быть вызваны для решения подзадачи z_i; M – множество информационных взаимодействий процессов, осуществляемых в ходе решения z_i; T_1 – множество функций интерпретаций терминов (концептов), используемых для представления сведений предметной области подзадачи z_i; T_2 – совокупность механизмов объяснения хода решения подзадачи z_i.

Каждая подзадача $z_i \in Z$ закрепляется за агентом a_i из агентного множества A. Имя агента может не совпадать с идентификатором подзадачи.

Наличие у агента механизма целеполагания *GOAL* обеспечивает ему принципиально новый уровень автономии. Агент не обязательно выполняет поручения пользователя или какого-либо другого агента, а просто зависит от условий среды выполнения, включая цели других агентов.

В отличие от объекта в объектно-ориентированном программировании и концепции *Object Management Group (OMG)* распределения объектов агент может принять на себя определенные обязательства или, наоборот, отказаться от таковых, мотивируя это отсутствием компетентности или недостатком ресурсов. Целеполагание осуществляется в соответствии с приемлемым для заказчика множеством критериев оценки и способов их структурирования. Например, при ориентации на *CC*, множество критериев можно структурировать в соответствии с двумя требованиями к безопасности: функциональными и доверительными. Функциональные, в свою очередь, можно представить тремя группами и одиннадцатью классами, а доверительные – двумя группами и десятью классами [1]. Цели (*GOAL*) не должны быть логически противоречивы.

Множество *H* в (1) представляет собой совокупность сведений, необходимых агенту для решения *i*-й подзадачи. Эти сведения могут находиться как в общей базе знаний мультиагентной системы, так и в локальных базах знаний отдельных агентов из *A*. Организация хранения и механизм обработки H_i определяет адекватную архитектуру агента $a_i \in A$ (например, продукционную, Холланда, *BDI*, с трехуровневой базой знаний) и мультиагентной системы в целом (как правило делиберативную) [2].

Множество *S* включает в себя методы, планы, сценарии, решения подзадач, в том числе «базовые» и «производные» процедуры. *К* «базовым» будем относить процедуры, имеющие известные алгоритмические схемы решения, а к «производным», напротив, нестандартные, заранее не предусмотренные способы решения. Выбор конкретного базового метода во многом предопределяется не только характером решаемой подзадачи z_i, но и формой представления сведений в *H* (числовые, символьные, нечеткие, вербализованные). В качестве примера рассмотрим возможный вариант метода оценки информационной безопасности, в котором критерии оценки интерпритируются как нечеткие суждения.

Пусть множество подзадач $\{z_i\}$ характеризуется набором критериев $x = \{x_1, ..., x_p\}$, каждый из которых является лингвистической переменной, заданной на базовом множестве *Z*. Подмножество из нескольких критериев характеризует представление агента о приемлемости принимаемого решения. Каждому подмножеству критериев поставим в соответствие значение переменной *R*, которая так же является лингвистической переменной, характеризующей «приемлемость» или «удовлетворительность» решения в целом. Тогда нечеткие суждения о решениях можно представить в виде следующих продукций:

$$P_i : (x_1 = C_{1i}) \cap (x_2 = C_{2i}) \cap ... \cap (x_p = C_{pi}) \to R = B_i , \quad (2)$$

где C_i – нечеткое множество базового множества *Z*; B_i – нечеткое множество единичного интервала *I*.

Выразим материальную импликацию (2) через оперции нечеткой логики:

$$\mu_E(z,i) = \min(1, (1 - \mu_C(z) + \mu_B(z)) , \quad (3)$$

где *E* – нечеткое подмножество на декартовом произведении $Z \times I, z \in Z, i \in I$; $\mu_E(z,i)$ – функция принадлежности (*z*, *i*) нечеткому множеству E.

Таким образом, продукции P_1, …, P_k вида (2) преобразуются в E_1, …, E_k. Общее функциональное решение подзадачи находится путем вычисления множества *E*:

$$E = E_1 \cap E_2 \cap ... \cap E_k . \quad (4)$$

Для каждой пары $(z,i) \in Z \times I$ в этом случае имеем

$$\mu_E(z,i) = \min\left(\mu_{EJ}\left(z, j\right)\right); j = \overline{i,k}, z \in Z . \quad (5)$$

Тогда «удовлетворенность» решения в целом можно оценить на основе композиционного правила вывода:

$$D_k = G_k \circ E , \quad (6)$$

где D_k – степень «удовлетворенности» *k*-ой оценки (нечеткое подмножество интервала *I*); G_k – отображения *k*-й оценки в виде нечеткого множества *Z*; *E* – функциональное решение.

В общем случае, каждый агент $\alpha_i \in A$ должен иметь библиотеку планов (сценариев) определяющих варианты ее возможных действий, связанных с решением задач, подобно рассмотренной. Решение подзадач возлагается на сервисы – программные компоненты, которые динамически взаимодействуют друг с другом с помощью стандартных протоколов *(XML, XSD, SSOAP, WSDL, HTTP)*. Планы и сервисы реализуют процедурные знания агентов. Планы должны содержать, по крайней мере, следующие четыре компонента: условие вызова (триггер), контекст (предусловие), главные условия и основное тело.

Условие определяет обстоятельства, при которых план рассматривается как возможный вариант. Предусловие разрешает запуск плана, а главное условие, по существу, контролирует выполнение основного тела.

Как уже отмечалось, сервисы, вызываемые в процессе выполнения плана, могут быть структурированы различными способами. Например, если ориентироваться на *CC*, то можно выделить три группы сервисов. Так при оценке функциональной безопасности, первая группа представлена сервисами оценивающими аудит безопасности (*FAU*), идентификацию и аутентификацию (*FIA*), а так же использование ресурсов (*FRV*). Производные сервисы включают оценку безопасности связи (*FCO*), приватности (*FPR*), защиты пользовательских данных (*FDP*), и защиты функций безопасности объекта (*FPT*). Наконец, третья группа сервисов связана с инфраструктурой оцениваемой системы. Она включает оценку криптографической поддержки (*FCC*), оценку управления безопасностью (*FMT*), оценку доступа к объекту (*FTA*) и оценку доверенного маршрута (*FTP*).

Предусловие запускает план агента только в случае получения необходимых сведений от других агентов по решению подзадачи. Такая процедура $m_i \in M$ по существу является операцией сбора сведений (single-node gather). Вариант информационного взаимодействия агентов для каждой подзадачи реализуется с помощью процедуры обобщенного сбора (multi-node gather). Указанная процедура может быть реализована на уровне локальных и глобальных, структурных и произвольных, статических и динамических схем информационного взаимодействия [3]. Минимизация информационных обменов между агентами обычно противоречит условию их равномерной загрузки. Например, нельзя разместить все нагрузки у одного агента и полностью устранить межагентную передачу сведений, хотя загрузка большинства агентов в этом случае будет минимальной. Решение вопросов сбалансированности нагрузки значительно усложняется, если планы агентов меняются в ходе решения подзадач. Один из вариантов динамического управления распределением нагрузки можно осуществить, например, с помощью схемы «manager worker»[4].

Децентрализация управления связана с ориентацией на самоорганизацию агентов, включая координацию, кооперацию, конкуренцию и коммуникацию. Такая форма взаимодействия агентов приводит к достижению совместной цели и выполнению действий при одновременном разделении между ними функций и обязательств. Эффективность согласованных действий агентов зависит от их групповой совместимости. Групповая совместимость должна образовывать иерархию уровней в мультиагентной системе. Нижним уровнем является типологическая совместимость (совместимость агентов разной типологии). На более высоком уровне групповая совместимость должна выступать как согласованность функционально-ролевых представлений агентов, в соответствии с результатами декомпозиции задачи оценки на подзадачи (1). Высший уровень характеризует мультиагентную систему как социум агентов.

Коммуникационные возможности агентов проявляются в ходе общения (путем обмена сведений *H*), отдельные аспекты которого реализуются побудительными, информационными и фактическими сообщениями. В рамках рассматриваемого формализма к побудительным относятся убеждения (архитектура *BDI*) и приказы (схема «manager worker»), к информационным – семафоры (при управлении доступом к разделяемым ресурсам), сведения отображающие содержание (illocution), следствия (perlocution) и перфоматив (performative) – глагол, употребление которого в первом лице настоящего времени означает непосредственное совершение определенного действия. А это значит, что множество *H* в (1) должно включать, по крайней мере, два типа сообщений: запросы и утверждения, а информационные взаимодействия *M* – два типа действий посылки и прием. Таким образом, реализуются фактические свойства агентов: респондентность и реципиентность.

Для обеспечения эксплицитности содержимого баз знаний и прозрачности мультиагентной системы необходимо поддерживать интерпретирующую – T_1 и объяснительную – T_2 функции [5]. В случае продукционной архитектуры агентов процедурная интерпретация правил «Если A, то B» может быть «от фактов» (добавление в базу знаний факта A вызывает добавление в нее и факта B) либо «от цели» (для достижения цели B делается попытка достичь цель A). Кроме того, так же, как в случае простейшей онтологии, множества терминов баз знаний X желательно представить в виде двух подмножеств X_1 и X_2:

$$X = X_1 \cup X_2, X_1 \cap X_2 = \emptyset, \tag{7}$$

где X_1 – совокупность интерпретируемых терминов; X_2 – совокупность интерпретирующих терминов.

Тогда

$$\exists(x \in X_1, y^1, y^2, ..., y^k \leftarrow X_2) \Rightarrow x = f(y^1, y^2, ...y^k). \tag{8}$$

Вид отображения f из T_1 определяет выразительную мощность и практическую полезность соответствующей интерпретации.

Множество T_2 реализуется средствами программ – трассировщиков [6], которые либо шаг за шагом, либо целиком прослеживают ход решения соответствующих подзадач, отвечая на вопросы «почему?» и «как?» было получено то или иное решение, обеспечивая тем самым «прозрачность» системы в целом. Таким образом, задание параметров в (1) по существу определяет адекватную типологию и архитектуру агентов, а также указывает на подходящую организационную структуру разрабатываемой мультиагентной системы.

Совместная деятельность агентов в рассматриваемом подходе должна характеризоваться высокой активностью, установлением многообразных межагентных отношений, мотивированностью и коллективным принятием решений. Высокая активность является характеристикой надситуативности, т. е. выхода за пределы исходных целей в отличие от приспособительности как ограничения действий агента узкими рамками заданного. Надситуативность, собственно, выступает как проявление интеллектуальности агента. Это обстоятельство становится особенно значимым в условиях оперативной коррекции показателей и критериев оценки или многократного изменения условий проведения мероприятий по оценке информационной безопасности систем.

ЗАКЛЮЧЕНИЕ

Таким образом, необходимо отметить, что предлагаемое представление задачи оценивания информационной безопасности системы в виде коннектора (1) позволяет трансформировать пространство состояний задачи и механизм ее решения в адекватную мультиагентную среду с элементами самоорганизации и коллективного взаимодействия системных единиц.

СПИСОК ЛИТЕРАТУРЫ

[1] **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 с.

[2] **Hiroaki Kitano.** Hendler Massively Parallel Artificial Intelligence, AAAI Press / Hiroaki Kitano and James A. // The MIT Press Menlo Park, California, Cambridge Massachusetts, 1995. – 426 с.

[3] **Москаленко Ю.С.** Организация систем, основанных на знаниях. учеб. пособие / Ю.С. Москаленко. – Издательский дом «Дальневосточный федеральный университет», г. Владивосток, 2013. – 250 с.

[4] **Рассел С.** Искусственный интеллект. Современный подход / С. Рассел, П. Норвиг. – Вильямс, 2005. –1408 с.

[5] **Люгер Дж.Ф.** Искусственный интеллект: Стратегии и методы решения сложных проблем / Дж.Ф. Люгер. – Вильямс, 2005. – 864 с.

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

REFERENCES

[1] 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.

[2] Hiroaki Kitano and James A. Hendler Massively Parallel Artificial Intelligence, AAAI Press / The MIT Press Menlo Park, California, Cambridge Massachusetts, 1995, 426 p.

[3] Moskalenko Y.S. Representation and processing of knowledge in training systems, School-book, Vladivostok, 2013, 250 p.

[4] Stuart Russell and Peter Norvig. Artificial Intelligence. Modern method. Williams, 2005, 1408 p.

[5] George F. Lyuger Artificial Intelligence: Strategies and methods for solving complex problems. Williams, 2005, 864 p.

[6] Kostrov B.V., Ruchkin V.N., Fulin V.A. Basics of artificial Intelligence, DESS, 2007, 192 p.

Варлатая Светлана Климентьевна, кандидат технических наук, профессор кафедры информационная безопасность Дальневосточного федерального университета. Основное направление научных исследований – исследования в области информационной безопасности. Имеет более 15 публикаций. E-mail: varlataya. sk@dvfu. ru.

Москаленко Юрий Сергеевич, кандидат технических наук, профессор кафедры информационная безопасность Дальневосточного федерального университета. Основное направление исследования – искусственный интеллект и технологии. Имеет 21 публикацию. E-mail: moskalenko. ys@dvfu. ru.

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

S.K. Varlataya, Y.S. Moskalenko, S.V. Shiryaev

Agent-based method to the assessment of corporate systems information security

The problems of development of smart tools of information security systems assessment on basis of multiagent technology are discussed in the article. The general method for assessment security of computer system on basis of security policy analysis with particular selection of showing of system immunity by method to determine and establish their values, and their comparison with pattern was proposed. In the paper are used the method for formalization and structuring of problem domain as multiagent system, which based on agent-orienteering technology using a intelligent agents as high-level abstraction. It shown, that intelligent agent must have possibility for interaction with user for production relevant tasks and return a results. The developed method, considering requirements based on unification of criteria and methods of information security assessment, enables to quickly correct decisions on changes in the descriptions of events at the expense of flexibility and autonomy of agents, regardless of the method of assessment. As an example, the article discusses possible option of information security assessment when criteria of assessment are interpreted as indistinct judgments. The possibility of quickly correct parameters and assessment criteria when you repeatedly change the conditions of the assessment activities in information security was shown. It considered problems of goal setting, managment knowledge base and planning of agent behavior. It analysised a patterns of information interaction of agents, decision subtasks on service level, ways of ensuring explicitness of content of knowledge bases and interpretability of the solving subproblems.

Key words: information security, assessment of security, criteria, space of status, status correction, intelligent agent, multiagent system, knowledge base, servises, agent architecture, social behavior of agent.