8 МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.491, 004.056.5

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОТКРЫТЫХ РАСПРЕДЕЛЕННЫХ МУЛЬТИАГЕНТНЫХ ВИРТУАЛЬНЫХ БИЗНЕС-СРЕДАХ

А.В. Маслобоев

Рассмотрены основные проблемы и виды угроз информационной безопасности открытых проблемно-ориентированных распределенных мультиагентных информационных систем. Предложены различные подходы к обеспечению информационной безопасности в открытых мультиагентных виртуальных бизнес-средах, основанные на реализации системы с централизованным и децентрализованным управлением безопасностью мобильных агентов, а также имитационном моделировании поведения их активных программных компонентов (агентов). Разработаны принципы функционирования и общая структура системы информационной безопасности в открытой мультиагентной виртуальной бизнес-среде (ОМАВБС) развития инноваций.

Ключевые слова: информационная безопасность, распределенные мультиагентные системы, виртуальная бизнес-среда, имитационное моделирование.

Введение

Актуальность исследований в области распределенного искусственного интеллекта и мультиагентных систем (МАС), согласно работе [1], определяется сложностью современных организационных и технических систем, разнообразием, сложностью и распределенностью решаемых задач, огромными объемами потоков информации и высокими требованиями к времени обработки информации. Теоретические исследования в области МАС ведутся в основном по следующим направлениям: теория агентов; коллективное поведение агентов; архитектура агентов и МАС; методы, языки и средства коммуникации агентов; языки реализации агентов; средства поддержки миграции агентов по сети. Наибольшую сложность в теоретических исследованиях и практических реализациях современных МАС представляют вопросы, связанные с обеспечением информационной безопасности агентов и информационных ресурсов, которыми они оперируют, в открытых мультиагентных виртуальных средах. Обеспечение информационной безопасности является важной задачей, которую необходимо решать при разработке МАС, ориентированных на использование в различных областях.

Проблематика и угрозы информационной безопасности в открытых МАС

Проблема обеспечения информационной безопасности в МАС может быть рассмотрена в нескольких аспектах. Во-первых, необходимо обеспечить защиту узлов сети от скрытых атак вредоносных программ или агентов-шпионов. Во-вторых, требуется обеспечить защиту самих агентов от воздействия приложений, запущенных на узлах сети. В-третьих, необходимо обеспечить защиту агентов МАС от атак агентов-шпионов, мигрирующих между узлами сети. Первая проблема – защита узлов от атак агентов-шпионов – может быть успешно решена посредством применения методов жесткой аутентификации исполняемого программного кода агентов, контроля целостности кода программ-агентов и ограничения прав доступа либо к самим программам-агентам, либо к информации или сервисам, которые они предоставляют. Вторая проблема – информационная безопасность агентов – является одной из основных нерешенных на сегодняшний день задач. Причиной этому является существование большого множества вредоносных программ, которые могут несанкционированным образом воздействовать на процесс функционирования агентов и манипулировать конфиденциальной информацией, которой оперируют агенты. Решение третьей проблемы основывается на создании специальных протоколов безопасности обмена сообщениями между агентами в мультиагентной среде.

К основным угрозам информационной безопасности распределенных МАС относятся: несанкционированный пассивный перехват сообщений в процессе межагентных коммуникаций, нарушение целостности передаваемых по сети данных, несанкционированный доступ к данным, отказ в обслуживании (DDoS-атаки), перехват запросов с последующей их модификацией и воспроизведением, отказ от факта получения или отправления данных и т.д. Децентрализованный характер построения распределенных МАС, отсутствие единого центра, гетерогенность компонентов, потенциальная возможность коммуникации с любым узлом делают мультиагентную среду максимально уязвимой для любого вида из перечисленных угроз.

Существующие решения проблем информационной безопасности открытых МАС

Обеспечение информационной безопасности рассматриваемого класса систем может быть организовано в виде комплекса известных решений. Наиболее эффективными и гибкими на сегодняшний день методами решения задач обеспечения информационной безопасности агентов и МАС являются: 1) метод защищенных состояний агентов [2]; 2) методы мобильной криптографии [3]; 3) модель безопасности Ксюдонга (POM Security Model) [4]; 4) модель безопасности Бадди (Buddy Security Model) [5]; 5) методы организации систем доверительных самоорганизующихся отношений [6]; 6) методы, основанные на использовании алгоритмов конфиденциальной связи и прокси-сервера, выполняющего функции ограничения и разграничения доступа к ресурсам и сервисам на основе методов идентификации и аутентификации [7]. Несмотря на столь широкий спектр существующих решений, ни один из перечисленных подходов не обеспечивает комплексного решения проблем информационной безопасности агентов от воздействия вредоносных узлов и программ-шпионов в открытых МАС.

Формальное представление ОМАВБС

В рамках настоящей работы решение проблемы информационной безопасности агентов и МАС рассматривается на примере задачи обеспечения информационной безопасности в ОМАВБС развития инноваций. С точки зрения общей логики функционирования виртуальная бизнес-среда имеет мультиагентную реализацию. Агентная ориентированность выражается в том, что в ней каждый реальный субъект инновационной деятельности представлен одним или несколькими мобильными программными агентами, которые представляют бизнес-предложения своих владельцев и реализуют процедуры автоматизированного поиска бизнес-партнеров для сотрудничества.

В общем случае модель ОМАВБС может быть задана в виде теоретико-множественных отношений и представляет собой следующий набор множеств:

$$OMAS = \{S, A, U, VBP, IR, O, ATR\},$$

где S – множество пользователей системы (субъектов бизнеса); A – множество агентов системы, представляющих интересы пользователей (их бизнес-предложения) в виртуальной бизнес-среде; $U = \{SH, KH\}$ – множество узлов системы, на которых функционируют агенты, причем SH – множество серверных хостов, а KH – множество клиентских хостов; VBP – множество виртуальных бизнес-площадок (ВБП), в пределах которых объединяются агенты совместной деятельности с близкими интересами и целями; IR – множество информационных ресурсов системы; O – отношения на множествах объектов модели; ATR – множество атрибутов объектов модели.

В системе функционируют агенты $A = \{MA, UA\}$ двух основных типов: MA – мобильные агенты, мигрирующие между узлами сети, и UA – управляющие агенты (агенты-модераторы), функционирующие в пределах ВБП и координирующие процессы взаимодействия и миграции мобильных агентов.

На множестве объектов модели могут быть заданы следующие отношения, определяющие структуру ОМАВБС:

$$O = \{SMA, SHVBP, MAVBP, UAVBP, UAMA\},$$

где $SMA \subset S \times MA$ – отношение наличия у каждого субъекта бизнеса своего виртуального представителя – агента; $SHVBP \subset SH \times VBP$ – отношение существования на каждом серверном узле системы ВБП; $MAVBP \subset MA \times VBP$ – отношение существования на каждой ВБП агентов совместной деятельности с общими областями интересов; $UAVBP \subset UA \times VBP$ – отношение принадлежности каждой виртуальной площадке своего управляющего агента (агента-модератора); $UAMA \subset UA \times MA$ – отношение принадлежности каждому управляющему агенту множества агентов совместной деятельности, взаимодействие которых он координирует.

Каждый мобильный агент описывается следующим набором параметров:

$$MA = \{ID_{MA}, ID_{MP}, ST, D_{MA}, SS\},$$

где ID_{MA} – уникальный идентификатор мобильного агента; ID_{MP} – уникальный идентификатор серверного узла, с которого мигрирует мобильный агент; ST – множество состояний мобильного агента; $D_{MA} \subset IR$ – множество данных, которыми оперирует мобильный агент; $SS = \{P, OK, ZK\}$ – внутренняя система безопасности мобильного агента; P – множество криптографических методов шифрования данных с открытым и/или закрытым ключом; OK – открытый ключ, известный только мобильному агенту и его управляющему агенту (частота обновления открытых ключей мобильных агентов определяется управляющим агентом); ZK – закрытый (секретный) ключ, известный только мобильному агенту (частота обновления секретного ключа определяется мобильным агентом), которым он подписывает свои запросы и данные.

Решение задачи обеспечения информационной безопасности в ОМАВБС

Новизна предлагаемого в настоящей работе решения задачи обеспечения информационной безопасности в открытых распределенных МАС заключается в комбинации двух подходов к формированию ОМАВБС, предложенных в работах [8, 9].

Первый подход основан на концепции закрытой сети «Closed Network» и заключается в формировании в мультиагентной виртуальной бизнес-среде независимых друг от друга агентных платформ (виртуальных площадок) на основе технологии [8], в пределах которых функционируют агенты с близкими интересами и целями (объединение агентов по интересам в закрытые «частные» группы), а также использовании метода защищенных состояний агентов [2] для предотвращения скрытых атак вредоносных программ и агентов-шпионов. Формирование ВПБ основано на методе поддержки распределенного реестра одноранговых узлов с неявной древовидной организацией [10] и осуществляется посредством отображения целей агентов на древовидные концептуальные модели предметной области. При этом ВБП может представлять собой либо выделенный узел в сети, либо группу узлов, образующих закрытую частную подсеть, либо часть адресного пространства агентного представительства (частная группа агентов по интересам), реализованного на каком-либо из узлов системы.

Предложенный второй подход, предпосылки которого изложены в работе [9], предполагает реализацию в открытой мультиагентной среде специализированного программного компонента – системы безопасности мобильных агентов (СБМА), обеспечивающей реализацию криптографических методов и механизмов защиты агентов системы от различного типа компьютерных атак со стороны вредоносных программ, а также использующей средства имитационного моделирования для анализа, прогнозирования и исследования динамики поведения агентов системы. В качестве средств моделирования могут быть использованы комплексы системно-динамических или агентных моделей. Для расширения функциональных возможностей СБМА в ее состав интегрированы разработанные специальные программные компоненты, обеспечивающие поддержку межагентного взаимодействия и самоорганизации агентов, а также реализующие механизмы защиты агентов системы от различного типа компьютерных атак со стороны вредоносных программ. К этим компонентам относятся: 1) реестр серверов; 2) сервер имен агентов; 3) сервер открытых ключей шифрования; 4) модуль шифрования данных; 5) специальный реестр «доска объявлений»; 6) система управления агентами. Реестр серверов содержит информацию о функционирующих узлах системы, а также контролирует подключение новых узлов и появление новых агентов в системе. Сервер имен агентов накапливает информацию об агентах системы. Формирование и поддержание распределенного реестра агентов осуществляется на базе их привязки к древовидным концептуальным моделям предметной области. Сервер открытых ключей совместно с модулем шифрования данных представляет собой ядро системы информационной безопасности агентов, агентных представительств и узлов системы. В нем реализуются процедуры идентификации и аутентификации агентов, а также криптографические методы защиты информации с открытым ключом. Сервер ключей хранит набор индивидуальных открытых ключей для шифрования информации, которой оперируют агенты системы при взаимодействии друг с другом и с приложениями, запущенными на узлах сети. В данной работе в качестве метода шифрования информации открытым ключом предложено использовать классический криптографический алгоритм асимметричного шифрования с открытыми ключами RSA и его модификации. Для обеспечения целостности и конфиденциальности своих запросов и защиты информации о бизнес-предложениях своих владельцев агенты используют электронную подпись и известные методы шифрования закрытым ключом. Специальный реестр «Доска объявлений» содержит информацию обо всех ВБП, зарегистрированных в системе, и входящих в их состав коалиций агентов. СБМА интегрируется с системой управления агентами, представляющей собой совокупность программных компонентов, реализующих внутреннюю логику функционирования и взаимодействия агентов, протоколы межагентных коммуникаций.

Логика функционирования СБМА

В ходе исследования предложены два варианта реализации СБМА: система с централизованным управлением безопасностью мобильных агентов и система с децентрализованным управлением безопасностью мобильных агентов.

В случае использования системы с централизованным управлением безопасностью мобильных агентов, СБМА в ОМАВБС реализуется на выделенном сервере. Сервер безопасности мобильных агентов обеспечивает централизованное хранение информации об агентах системы, доступных узлах, ВБП, открытых ключах агентов, доступ к которым имеют только управляющие агенты системы. Здесь же реализуются модули шифрования и дешифрования данных, а также система мониторинга, анализа и моделирования поведения агентов системы, которая также доступна управляющим агентам системы. Архитектура и логика функционирования ОМАВБС при таком подходе к реализации СБМА представлены на рис. 1.

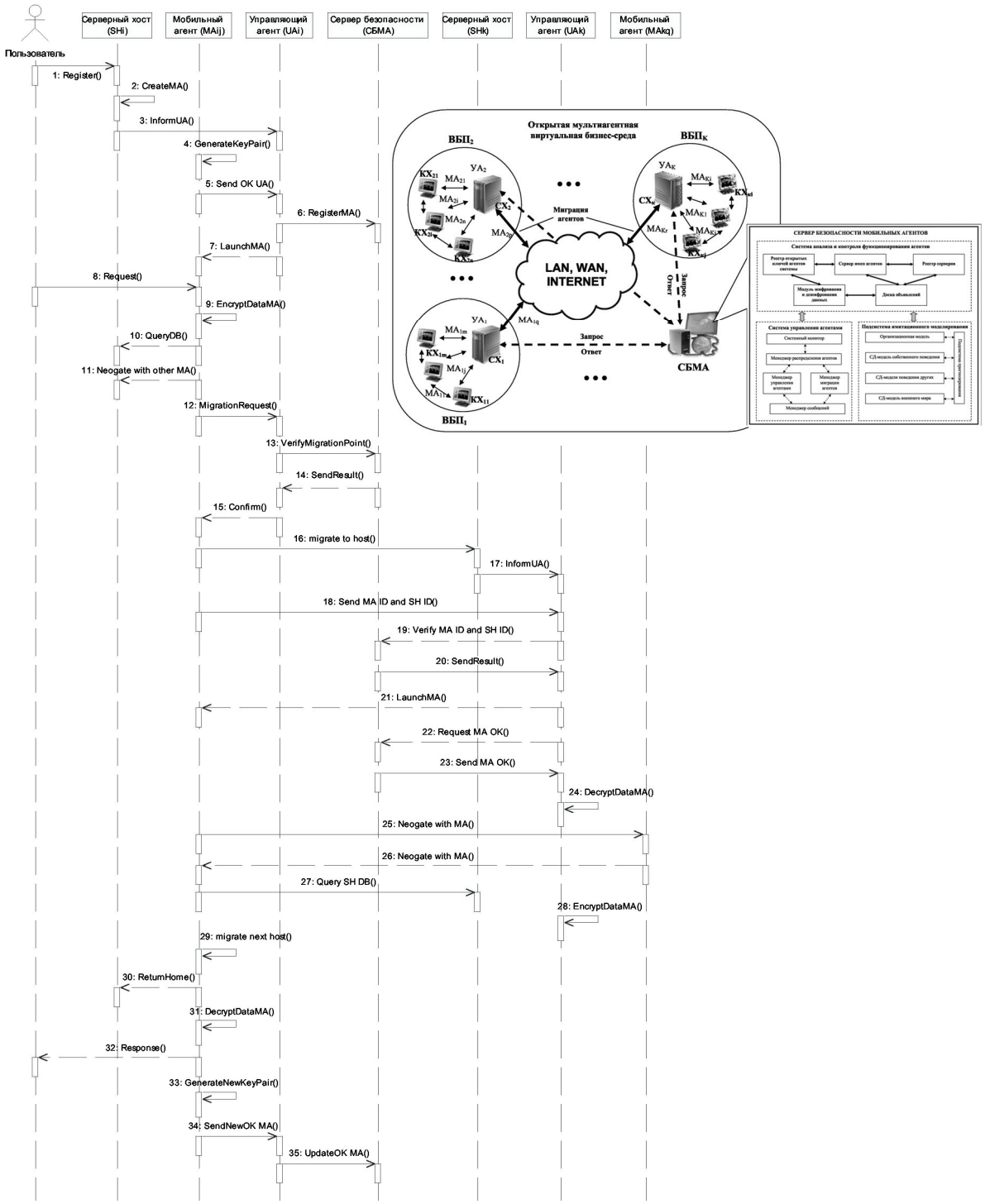

Рис. 1. Архитектура и логика функционирования ОМАВБС с системой централизованного управления безопасностью мобильных агентов

В случае использования системы с децентрализованным управлением безопасностью мобильных агентов СБМА в ОМАВБС реализуется на каждом из серверных узлов системы (порталов), на которых пользователи регистрируют свои бизнес-предложения. При таком решении СБМА является частью агентного представительства серверного узла и выполняет те же функции, что и сервер безопасности мобильных агентов: хранит информацию об агентах системы, доступных узлах, ВБП, открытых ключах агентов, доступ к которым имеют только управляющие агенты системы, реализует процедуры шифрования и дешифрования данных агентов, осуществляет мониторинг, анализ и моделирование поведения агентов системы. В этом случае часть функций по обеспечению безопасности возлагаются на управляю-

щих агентов ВБП. Архитектура и логика функционирования ОМАВБС при таком подходе к реализации СБМА представлены на рис. 2.

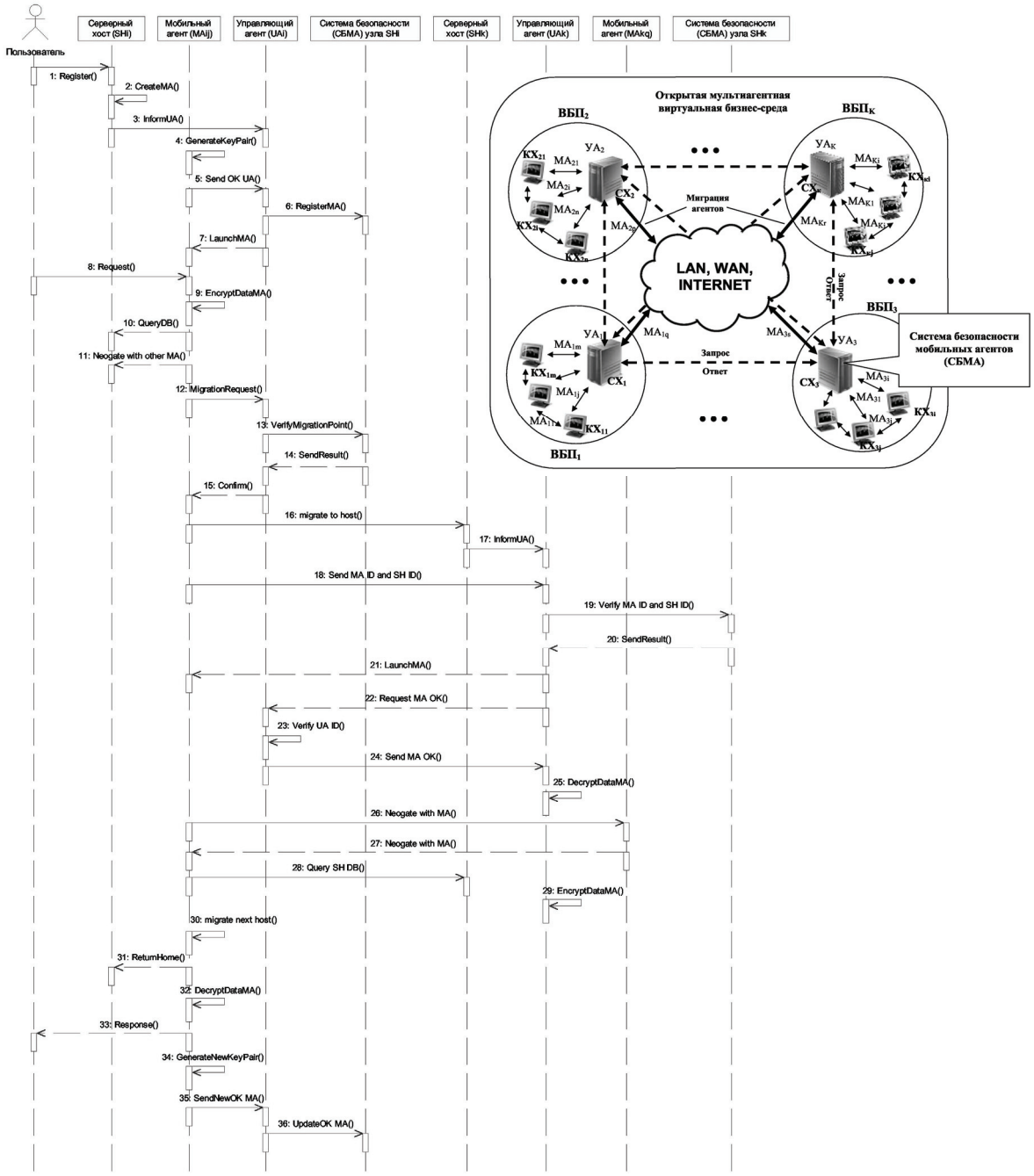

Рис. 2. Архитектура и логика функционирования ОМАВБС с системой децентрализованного управления безопасностью мобильных агентов

Очевидно, что реализация ОМАВБС с системой децентрализованного управления безопасностью (максимально возможный отказ от централизованных общесистемных сервисов обеспечения безопасности) повышает ее надежность и устойчивость к внешним и внутренним угрозам информационной безопасности, а также позволяет организовать эффективную защиту агентов и узлов системы от целенаправленного воздействия вредоносных программ и агентов-шпионов. Достоинствами данного варианта реализации СБМА, несмотря на достаточно высокую загрузку коммуникационных каналов и избыточность хранимых данных, являются также гибкость, адаптируемость и распределение нагрузки по обеспечению информационной безопасности между серверными узлами системы и управляющими агентами.

Несмотря на ряд достоинств системы с централизованным управлением безопасностью, также присущим распределенным информационным системам с централизованной архитектурой, можно отметить основные проблемы систем подобного типа, к которым можно отнести: 1) уязвимость центрального

звена (при отказе сервера безопасности нарушается защита активных компонентов и всей системы в целом, ее безопасность ставится под угрозу); 2) высокая нагрузка на центральный сервер управления безопасностью при большом количестве агентов и узлов и, как следствие – ограниченная масштабируемость; 3) централизованное администрирование, которое подразумевает полный контроль над ресурсами на стороне сервера, что не всегда приемлемо, если ресурсы принадлежат разным пользователям.

Заключение

В ходе проведенных исследований проанализированы основные проблемы и виды угроз информационной безопасности открытых проблемно-ориентированных распределенных мультиагентных информационных систем. Разработаны принципы функционирования и общая структура системы информационной безопасности в ОМАВБС. Предложены различные подходы к обеспечению информационной безопасности в ОМАВБС, основанные на реализации системы с централизованным и децентрализованным управлением безопасностью, а также имитационном моделировании поведения их активных компонентов (агентов). Предложенные подходы составляют основу подсистемы информационной безопасности, реализованной в виде комплекса программ в рамках системы информационной поддержки инновационной деятельности, представляющей собой ОМАВБС инноваций. Мобильные программные агенты и предложенные механизмы управления информационной безопасностью реализованы в программной инструментальной среде разработки агентов и MAC JADE (Java Agent Application Environment).

Литература

1. Рыбина Г.В., Паронджанов С.С. Модели, методы и программные средства поддержки взаимодействия интеллектуальных агентов // Информационные технологии и вычислительные системы. – М.: УРСС, 2008. – Вып.3. – С. 22–29.
2. Neeran K.M., Tripathi A.R. Security in the Ajanta MobileAgent System // Technical Report. – Department of Computer Science, University of Minnesota, May 1999.
3. Sander T., Tschudin Ch.F. Protecting MobileAgents Against Malicious Hosts. In Giovanni Vigna (ed.) // MobileAgents and Security, LNCS, Springer, 1998. – P. 44–60.
4. Xudong G., Yiling Ya., Yinyuan Y. POM-a mobile agent security model against malicious hosts // Proceedings of High Performance Computing in the Asia-Pacific Region. – 2000. – V. 2. – P. 1165–1166.
5. Page J., Zaslavsky A., Indrawan M. A Buddy model of security for mobile agent communities operating in pervasive scenarios // Proceeding of the 2nd ACM Intl. Workshop on Australian Information Security & Data Mining. – 2004. – V. 54.
6. Ramchurn S.D., Huynh D., Jennings N.R. Trust in multi-agent systems // The Knowledge Engineering Review. – Cambridge University Press New York, NY, USA, 2004. – V. 19. – Is. 1 (March 2004). – P. 1–25.
7. Min-Hui L., Chin-Chen Ch., Yan-Ren Ch. A fair and secure mobile agent environment based on blind signature and proxy host // Journal of Computer and Security. – 2004. – № 23(4). – P. 199–212.
8. Маслобоев А.В. Мультиагентная технология формирования виртуальных бизнес-площадок в едином информационно-коммуникационном пространстве развития инноваций // Научно-технический вестник СПбГУ ИТМО. – 2009. – № 6(64). – С. 83–89.
9. Kannammal A., Iyengar N.Ch.S.N. A Framework for Mobile Agent Security in Distributed Agent-Based E-Business Systems // International Journal of Business and Information. – 2008. – V. 3. – № 1. – P. 129–143.
10. Путилов В.А., Шишаев М.Г., Олейник А.Г. Технологии распределенных систем информационной поддержки инновационного развития региона // Труды Института системного анализа РАН. – М.: УРСС, 2008. – Т. 39. – С. 40–64.

Маслобоев Андрей Владимирович – Институт информатики и математического моделирования технологических процессов Кольского научного центра РАН, кандидат технических наук, доцент, докторант, masloboev@iimm.kolasc.net.ru