Вестник МГТУ, том 13, №4/2, 2010 г. стр.1015-1032

УДК 004.491, 004.056.5.

Разработка и реализация механизмов управления информационной безопасностью мобильных агентов в распределенных мультиагентных информационных системах

А.В. Маслобоев, В.А. Путилов

Институт информатики и математического моделирования технологических процессов КНЦ РАН

Аннотация. В работе рассматриваются проблематика и основные виды угроз информационной безопасности открытых проблемно-ориентированных распределенных мультиагентных информационных систем (ОМАС). Предложены подходы к обеспечению информационной безопасности в ОМАС, основанные на реализации механизмов централизованного и децентрализованного управления безопасностью мобильных агентов, а также имитационном моделировании поведения их активных программных компонентов (агентов). Разработан метод формирования комплексной самоорганизующейся системы децентрализованного управления безопасностью мобильных агентов в ОМАС, реализующей механизмы аутентификации агентов с помощью открытых ключей посредством удостоверяющих центров. Представлен сравнительный анализ реализованных систем безопасности мобильных агентов в зависимости от типа управления безопасностью в ОМАС. Разработаны вычислительные модели показателей эффективности (производительности) систем безопасности мобильных агентов с реализованными механизмами централизованного и децентрализованного управления безопасностью.

Abstract. In this paper the main information security problems and kinds of threats of the open problem-oriented distributed agent-based information systems (OMAS) have been considered. Approaches to information security support (protection) in OMAS based on mobile agent security system with centralized and decentralized control mechanisms implementation and pro-active software components (agents) behavior simulation have been proposed. A formation method for complex self-organized mobile agent security system with decentralized security control in OMAS, based on public key authentication mechanisms implementation via certificate authority has been developed. The comparative research of the implemented mobile agent security systems subject to security control modes has been represented. The mathematical models of the proposed mobile agent security systems functioning performance evaluation indicators have been developed.

Ключевые слова: информационная безопасность, распределенные мультиагентные системы, оценка эффективности функционирования, виртуальная бизнес-среда, управление безопасностью мобильных агентов

Key words: information security, distributed multi-agent systems, functioning performance evaluation, mobile agent security control, virtual business environment

1. Введение

Актуальность исследований в области распределенного искусственного интеллекта и мультиагентных систем (МАС), в соответствии с работами (*Рыбина, Пароджанов*, 2008) и (*Тарасов*, 2002), определяется сложностью современных организационных и технических систем, разнообразием, сложностью и распределенностью решаемых задач, огромными объемами информационных потоков 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. Мультиагентный подход находит широкое применение в различных областях, требующих решения сложных распределенных задач, таких как реинжиниринг бизнес-процессов, построение виртуальных предприятий, имитационное моделирование интегрированных производственных систем, электронная торговля, организация работы коллективов роботов и т.д. 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. Мобильные агенты являются автономными программными агентами, способными мигрировать между узлами сети в целях выполнения задач, поставленных перед ними их владельцами. Автономные агенты обеспечивают такие преимущества, как делегирование функций, сетевые коммуникации, снижение

нагрузки, увеличение производительности при решении комплексных распределенных задач. Обеспечение информационной безопасности является важной задачей, которую необходимо решать при разработке мультиагентных систем, ориентированных на использование в различных областях.

В статье рассмотрены основные проблемы и виды угроз информационной безопасности открытых проблемно-ориентированных распределенных мультиагентных информационных систем (ОМАС). В качестве объекта исследования рассматривается достаточно распространенная система подобного типа – мультиагентная система информационной поддержки инновационной деятельности (*Маслобоев, Шишаев*, 2009). Для таких систем характерны большие объемы и высокая скорость обрабатываемой информации, что делает критичной задачу обеспечения информационной безопасности. Представлены существующие модели и методы обеспечения информационной безопасности агентов и мультиагентных систем. Проведен анализ рисков информационной безопасности, характерных для данного класса систем, и выделены основные задачи, успешное решение которых приводит к уменьшению выявленных рисков. Предложены различные подходы к обеспечению информационной безопасности в ОМАС, основанные на реализации механизмов централизованного и децентрализованного управления безопасностью мобильных агентов, а также имитационном моделировании поведения активных программных компонентов (агентов) ОМАС. Предложенные в работе решения существенно расширяют возможности широко используемой на практике инфраструктуры безопасности PKI (Public Key Infrastructure) (*Полянская, Горбатов*, 2007), представляющей собой систему аутентификации пользователей с помощью открытых ключей посредством удостоверяющих центров (система безопасности на основе сертификатов), за счет реализации процедур автоматического формирования децентрализованных центров сертификации на основе методов самоорганизации активных программных компонентов открытых распределенных мультиагентных информационных систем (*Маслобоев*, 2009с).

2. Проблемы и угрозы информационной безопасности в ОМАС

Проблема обеспечения информационной безопасности в мультиагентных системах 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 мультиагентных систем 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 мультиагентных систем, отсутствие единого центра, гетерогенность компонентов, потенциальная возможность коммуникации с любым узлом делают мультиагентную среду максимально уязвимой для любого вида из перечисленных угроз (*Федоров, Датьев*, 2008).

3. Существующие решения проблем информационной безопасности в ОМАС

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 мультиагентных систем являются: 1) метод защищенных состояний агентов (*Neeran, Tripathi*, 1999); 2) методы мобильной криптографии (*Sander, Tschudin*, 1998); 3) модель безопасности Ксюдонга (POM Security Model) (*Xudong et al.*, 2000); 4) "товарищеская" модель взаимной безопасности (Buddy Security Model) (*Page et al.*, 2004); 5) методы организации систем самоорганизующихся доверительных отношений (*Ramchurn et al.*, 2004); 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 (*Min-Hui et al.*, 2004). Рассмотрим некоторые из них.

Метод защищенных состояний (*Neeran, Tripathi*, 1999) основан на электронной подписи и кодировании информации о состояниях агента посредством криптографических методов шифрования данных с открытым ключом. Метод обеспечивает конфиденциальность и целостность данных, которыми оперируют агенты системы. Для предотвращения угроз нарушения целостности данных агентов они переводятся в определенные состояния, например: состояние только для чтения данных агента, состояние только для модификации данных агента, состояние ограничения доступа к агенту со стороны других агентов и программ т.п. Этот метод является гибким и эффективным, т.к. базируется на современных достижениях научных исследований в области теории криптографии. Несмотря на это, этот метод не позволяет обеспечить целостность исполняемого программного кода и конфиденциальность агентов.

С помощью мобильной криптографии (*Sander, Tschudin*, 1998) можно достичь определенного уровня защиты целостности программного кода агентов. Пример использования методов мобильной криптографии для защиты исполняемого программного кода представлен далее. Если Клиенту необходимо чтобы Сервер вычислил для него некоторую функцию f, данные для которой хранятся на Сервере в переменной x, то Клиенту необходимо зашифровать функцию f для получения значения $E(f)$. Далее необходимо выполнить программу P, чтобы вычислить функцию $E(f)$ и переслать на Сервер программу P. Получив программу P, Сервер запустит ее на исполнение, но при этом он не сможет получить результат работы функции $f(x)$. Кроме того, он сможет получить всего лишь зашифрованный результат работы $E(f(x))$, который сможет прочитать только Клиент, т.к. у него имеется ключ для дешифрования этих данных. Более того, Сервер не может модифицировать процесс выполнения программы P, т.к. она реализована на основе зашифрованной функции f, закрытой от Сервера. Такой вид шифрования пригоден только для полиноминальных функций. Однако если бы методы мобильной криптографии могли быть расширены для других типов функций, так, чтобы любая функция смогла шифровать данные и вычислялась бы на удаленном хосте, то всецело можно было бы решить проблему "опасных" узлов.

Метод Ксюдонга (*Xudong et al.*, 2000) основывается на следующем подходе. В каждую область мультиагентной системы, по аналогии с реальным миром, вводится дополнительный управляющий узел, который отвечает за всю безопасность данной области. Разбиение на области осуществляется случайным образом. В концепции Ксюдонга этот узел принято называть полицейским участком (PO – Police Office), а модель управления безопасностью, основанную на его использовании, называют POM (Police Office Model – модель обеспечения безопасности на основе полицейских участков). Любой агент, которому необходимо мигрировать на некоторый узел, входящий в состав какой-либо из областей MAC, должен быть зарегистрирован в агентном представительстве узла PO своей области. В модели безопасности Ксюдонга агенты системы имеют одинаковую структуру, но могут обладать различными функциональными возможностями. Структура мобильных агентов состоит из двух частей: основная (master part) и дополнительная (slave part) части. Основная часть является секретной частью агента, а дополнительная – открытой частью агента. В процессе миграции агентов между узлами, принадлежащими разным областям, по сети перемещается не весь исполняемый программный код агента и его данные целиком, а только его дополнительная часть (slave part). Перед тем, как мигрировать на какой-либо узел сети, принадлежащий другой области, агент перемещается на узел PO своей области, где его основная часть активизируется и после некоторых секретных операций отделяется от дополнительной части. Далее инициируется пересылка дополнительной части агента на заданный узел системы для сбора необходимой информации. После того, как необходимая информация была собрана, дополнительная часть агента возвращается на узел PO своей области. Если основная часть агента идентифицировала какие-либо подозрительные действия (изменения) над своей дополнительной частью, то она оповещает об этом агентное представительство узла PO, которое, в свою очередь, определяет дальнейшие стратегии взаимодействия с узлом, с которого мигрировала обратно дополнительная часть агента. Если целостность дополнительной части агента не вызывает подозрений, то основная часть агента определяет следующий узел, на который данному агенту необходимо мигрировать и осуществить сбор данных.

"Товарищеская" модель взаимной безопасности (*Page et al.*, 2004) представляет собой такую систему безопасности, в рамках которой агенты отвечают за безопасность друг друга, отслеживая происходящие в системе события взаимодействуя между собой и внешней средой. В агентно-ориентированных системах, в которых реализуется данная модель безопасности, все агенты имеют идентичную структуру, и отсутствуют управляющие агенты и/или узлы, поэтому невозможно атаковать какой-то центральный узел, отвечающий за всю безопасность MAC. Каждый агент в "товарищеской" модели взаимной безопасности "знает", что рядом есть другой агент, который в случае опасности "поможет" своему "товарищу". В процессе межагентных коммуникаций агенты системы обмениваются специальными сообщениями, которые несут в себе секретную информацию о состояниях известным им агентов и о возможных угрозах с их стороны, либо со стороны узлов сети. Таким образом, все агенты системы получают информацию о потенциальных угрозах их безопасности. Информируя своих соседей о

возможной опасности (например, при появлении "чужого" агента в системе), каждый из агентов несет ответственность за безопасность своего окружения и всей системы в целом.

Несмотря на столь широкий спектр существующих решений, ни один из перечисленных подходов не обеспечивает комплексного решения проблем информационной безопасности в ОМАС. Вместе с тем, вопросы, связанные с защитой агентов и информационных ресурсов, которыми они оперируют, от воздействия вредоносных узлов и программ-шпионов, остаются открытыми и недостаточно проработанными как в отечественной, так и в зарубежной практике исследования и анализа рисков информационной безопасности таких сложных объектов информатизации, как ОМАС.

В ряде работ (*Котенко*, 2009; *Городецкий и др.*, 2006; *Котенко, Уланов*, 2009) рассматривается использование интеллектуальных мультиагентных систем для защиты информации в одноранговых распределенных информационных системах. В частности, дается обзор инструментов реализации атак, способов формирования онтологии сетевых атак, определяются структура и состав команды агентов, специализирующихся на защите информации, выявлении и локализации угроз безопасности и т.д. Вместе с тем, обсуждаются вопросы применения мультиагентных и интеллектуальных технологий для обнаружения вторжений на серверные узлы компьютерных сетей, тестирования защищенности и обучения систем ИТ. Вместе с тем авторами этих работ предлагаются подходы к построению систем моделирования атак на узлы распределенных информационных систем, основанные на использовании онтологии сетевых атак, стратегий их реализации, а также применении хранилища уязвимостей и программ реализации атак.

4. Структура и состав открытой мультиагентной виртуальной бизнес-среды

Для решения проблем информационной безопасности в открытых мультиагентных системах необходимо создавать соответствующие проблемно-ориентированные модели и информационные технологии, учитывающие специфику их состава и структуры. В настоящей работы решение проблем информационной безопасности в ОМАС рассматривается на примере задачи обеспечения информационной безопасности в ОМАС информационной поддержки инноваций, реализующей открытую мультиагентную виртуальную бизнес-среду инновационной деятельности (ОМАВБС). Важной особенностью рассматриваемой ОМАС является ее открытость для свободного подключения и отключения новых агентов, а также способность функционирования в условиях большого количества входящих в систему узлов. Такая свобода и масштабируемость обеспечивается заложенными в систему механизмами равноправного (пирингового) взаимодействия узлов и функциональных компонентов. С точки зрения существующих разновидностей пиринговых архитектур, рассматриваемую ОМАС можно отнести к гибридным одноранговым системам. Современные ОМАС данного типа характеризуются не только разнородностью и территориальной распределенностью своих активных программных компонентов (агентов), вкупе с динамичностью их состава и параметров, но и гибкой расширяемостью, а также способностью к саморазвитию в условиях полного отсутствия или минимального объема внешнего управления.

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 виртуальных бизнес-площадок и координирующие процессы взаимодействия и миграции мобильных агентов.

На множестве объектов модели 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 виртуальных бизнес-площадок; $MAVBP \subset MA \times VBP$ – отношение "существования" на каждой виртуальной бизнес-площадке 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.

Структура данных мобильного агента описывается следующим множеством параметров:

$$D_{MA} = \{BP, AList, UList, VBPList, QList, RList\},$$

где BP – информация о бизнес-предложениях; $AList$ – адресная база зарегистрированных в системе агентов, известных мобильному агенту; $UList$ – реестр адресов узлов системы, известных мобильному агенту, на которые он может мигрировать; $VBPList$ – реестр адресов узлов системы, содержащих виртуальные бизнес-площадки, предметная ориентация которых совпадает с областью интересов мобильного агента; $QList$ – множество запросов мобильного агента; $RList$ – множество полученных результатов запросов мобильного агента.

5. Решение задачи обеспечения информационной безопасности в ОМАВБС

В качестве одного из эффективных решений задачи обеспечения информационной безопасности в открытых распределенных мультиагентных системах авторами статьи предлагается метод формирования комплексной самоорганизующейся системы децентрализованного управления безопасностью мобильных агентов, реализующей механизмы аутентификации агентов с помощью открытых ключей посредством удостоверяющих центров.

Логика работы такой системы управления безопасностью мобильных агентов во многом воспроизводит идеи, заложенные в концепцию систем информационной безопасности на основе сертификатов PKI (*Полянская, Горбатов*, 2007). Но, в отличие от последней, где изначально подразумевается, что процесс формирования центров сертификации и процедура выдача сертификатов реализуются на основе предварительных соглашений между пользователями, в предлагаемой системе формирование удостоверяющих центров будет осуществляться автоматически на основе механизмов самоорганизации агентов в ОМАС, а функции управления процедурой выдачи сертификатов будут возложены не на пользователей-администраторов удостоверяющих центров, а на их виртуальных представителей в ОМАС – программных управляющих агентов.

Самоорганизация в данном случае будет заключаться в автоматическом формировании в рамках ОМАС виртуальных площадок, объединяющих агентов с близкими целями в коалиции – частные сети агентов по интересам, и генерации управляющих агентов, выполняющих функции удостоверяющих центров сертификации, для каждой площадки. Управляющие агенты, взаимодействуя с себе подобными и остальными агентами ОМАС, помимо реализации функций управления информационной безопасностью, контролируют информационный обмен (переговоры) между агентами внутри подведомственных им площадок (сегментов сети).

Предлагаемый метод реализован на основе комбинирования двух подходов к формированию открытых мультиагентных виртуальных бизнес-сред, предложенных в работах (*Маслобоев*, 2009b) и (*Kannammal, Iyengar*, 2007).

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 (*Маслобоев*, 2009b), в пределах которых функционируют агенты с близкими интересами и целями (объединение агентов по интересам в закрытые "частные" группы), а также использовании рассмотренного выше метода защищенных состояний агентов (*Neeran, Tripathi*, 1999) для предотвращения скрытых атак вредоносных программ и агентов-шпионов. Формирование виртуальных бизнес-площадок основано на методе поддержки распределенного реестра одноранговых узлов с неявной древовидной организацией (*Путилов и др.*, 2008) и осуществляется посредством отображения целей агентов на древовидные концептуальные модели предметной области, последующей локализации основной части поисковых и иных запросов агентов внутри группы, и дальнейшего анализа активности их коммуникаций друг с другом. При этом виртуальная бизнес-площадка 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 авторами второй подход, предпосылки которого изложены в работе (*Kannammal, Iyengar*, 2007), 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 (*Cao, Fu*, 2008) или его модификации (*Peng, Wu*, 2008). 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 виртуальных бизнес-площадках, зарегистрированных в системе, и входящих в их состав коалициях агентов. Анализ информации, представленной на "Доске объявлений", позволяет оценить нагрузку на узлах системы и определить интенсивности межагентных и межгрупповых коммуникаций на межузловом и внутриузловом уровнях, что позволяет осуществить динамическое перераспределение агентов и групп агентов между узлами системы. СБМА интегрируется с системой управления агентами, представляющей собой совокупность программных компонентов, реализующих внутреннюю логику функционирования и взаимодействия агентов, протоколы межагентных коммуникаций.

6. Логика функционирования системы безопасности мобильных агентов

В ходе исследования предложены два варианта реализации СБМА: система с централизованным управлением безопасностью мобильных агентов и система с децентрализованным управлением безопасностью мобильных агентов. Рассмотрим их принципы функционирования по отдельности.

При подключении нового пользователя к системе для него создается его виртуальный представитель – мобильный агент *MA*, действующий в интересах пользователя. Агенты генерируются на серверных узлах системы *SH* и выполняют следующие основные функции: 1) поиск бизнес-предложений и/или бизнес-партнеров, удовлетворяющих заданным ограничениям, в информационных базах

распределенных разнородных серверных узлов; 2) формирование виртуальных бизнес-структур (коалиций агентов) для реализации конкретного бизнес-проекта. На агентов возлагаются не только задачи поиска и размещения информации, но и функции по ее анализу и обработке. Агент предоставляет собранную и сформированную информацию своему владельцу для принятия решения.

После генерации нового агента в системе информация о нем и о его владельце регистрируется в соответствующих системных реестрах. Каждому новому агенту в момент создания управляющим агентом *UA* присваивается уникальный идентификатор ID_{MA} и имя, которые регистрируются на сервере имен агентов, а также определяется открытый ключ OK_{MA} для шифрования/дешифрования данных D_{MA} агента. Секретный ключ ZK_{MA} генерируется самим агентом в момент регистрации в системе. Открытый ключ известен только управляющему агенту "родного" узла системы, где был создан агент *MA*. После прохождения этапа регистрации в системе вновь созданный агент, взаимодействуя с другими агентами в пределах агентного представительства того узла сети, где он был сгенерирован, пополняет свои знания о системе, а именно собирает информацию о зарегистрированных в системе агентах, узлах системы и виртуальных бизнес-площадках, проблемная ориентация которых совпадает с областью его интересов.

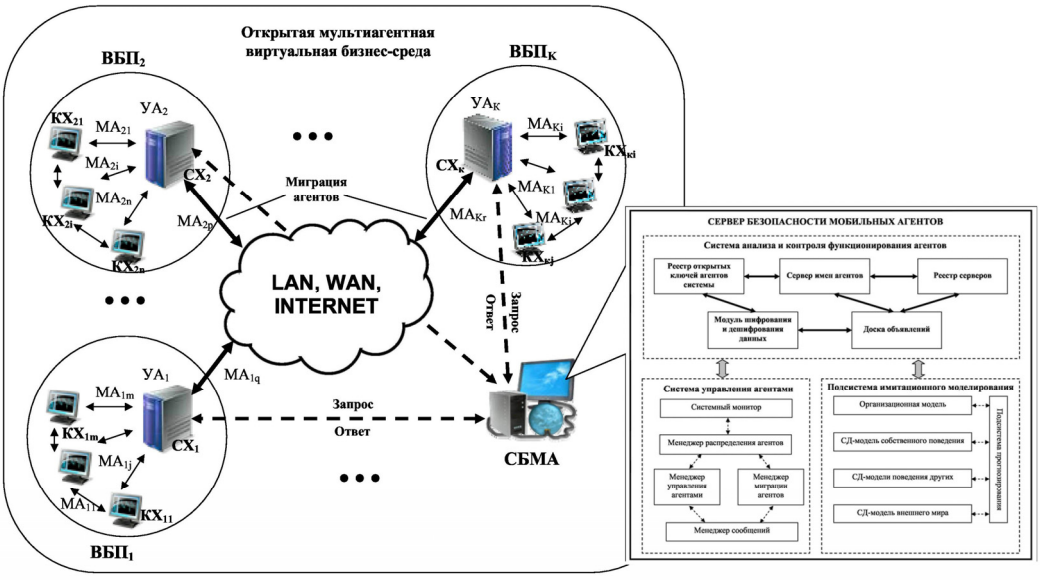

Рис. 1. Открытая мультиагентная виртуальная бизнес-среда с системой централизованного управления безопасностью мобильных агентов
(СБМА – система безопасности мобильных агентов; ВБП – виртуальная бизнес-площадка; МА – мобильный агент; УА – управляющий агент; СХ – серверный хост; КХ – клиентский хост)

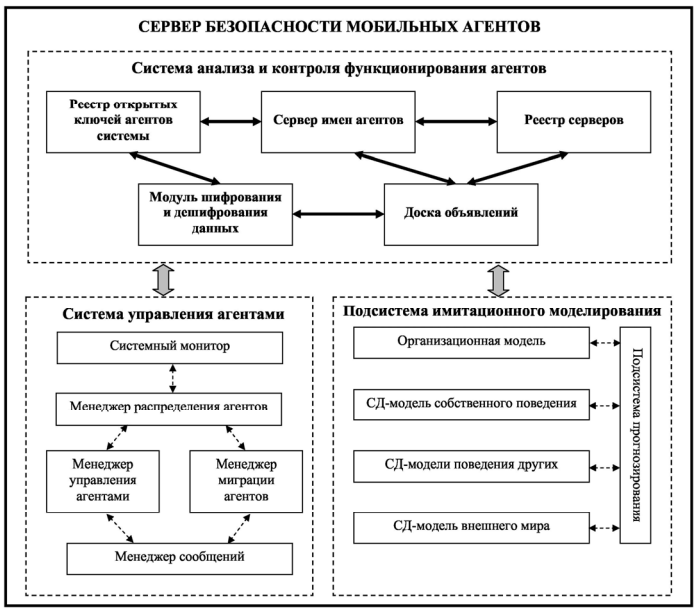

Рис. 2. Функциональная структура сервера безопасности мобильных агентов

В случае использования системы с централизованным управлением безопасностью мобильных агентов (рис. 1) СБМА в открытой мультиагентной виртуальной бизнес-среде реализуется на выделенном сервере, функциональная структура которого представлена на рис. 2. Сервер безопасности мобильных агентов обеспечивает централизованное хранение информации об агентах системы, доступных узлах, виртуальных бизнес-площадках, открытых ключах агентов, доступ к которым имеют только управляющие агенты системы. Здесь же реализуются модуль шифрования и дешифрования данных, а также система мониторинга, анализа и моделирования поведения агентов системы, которая также доступна управляющим агентам системы. Рассмотрим логику функционирования основных компонентов ОМАВБС при таком подходе к реализации СБМА (рис. 3).

Предположим, что некоторый мобильный агент MA_{i1} планирует мигрировать с виртуальной бизнес-площадки VBP_i, расположенной на узле SH_i, на виртуальную бизнес-площадку VBP_k, функционирующую на узле SH_k. Агент MA_{i1} отправляет запрос своему управляющему агенту UA_i на осуществление миграции на VBP_k узла SH_k. Управляющий агент UA_i, получив запрос от агента MA_{i1}, обращается к серверу безопасности мобильных агентов, выполняющему функции головного удостоверяющего центра, запрашивая информацию для проверки существования SH_k и VBP_k соответственно. В случае положительного ответа управляющий агент UA_i разрешает агенту MA_{i1} осуществить миграцию на узел SH_k и инициирует процесс перемещения агента MA_{i1} с помощью менеджера миграции агентов. На входе в агентное представительство узла SH_k, представляющем собой защищенную область памяти (внешняя среда агентного представительства принимающего узла), куда загружаются программный код и данные мигрирующего агента и доступ к которой имеют только управляющие агенты принимающего узла SH_k, агент MA_{i1} предъявляет управляющему агенту UA_k площадки VBP_k, членом которой он хочет стать, свой сертификат, представляющий собой электронный документ, который содержит электронный ключ агента, информацию об агенте (уникальный идентификатор ID_{MAi1}, идентификатор (адрес) ID_{MPi} серверного узла, с которого он мигрировал и т.д.), удостоверяющую подпись центра выдачи сертификатов UA_i и информацию о сроке действия сертификата. Управляющий агент UA_k площадки VBP_k обращается к центральному серверу безопасности мобильных агентов и осуществляет проверку данных, содержащихся в сертификате агента MA_{i1}. Если такой агент и узел зарегистрированы в системе и сертификат является подлинным, то агент MA_{i1} загружается в основную память узла SH_k, а ресурсы узла SH_k в пределах адресного пространства площадки VBP_k становятся доступными агенту MA_{i1}. Агент MA_{i1} может собирать нужную информацию и вступать в переговоры с агентами, принадлежащими площадке VBP_k. В противном случае, агент MA_{i1} блокируется, а доступ к ресурсам узла SH_k для него запрещается. Вместе с тем, управляющий агент UA_k заносит агента MA_{i1} в "черный список" и информирует всех известных ему агентов о присутствии "чужого" агента в системе.

Так как все данные D_{MAi1}, которыми оперирует агент MA_{i1}, зашифрованы закрытым ключом, который неизвестен ни одному из агентов в пределах узла SH_k, управляющий агент UA_k обращается к серверу безопасности мобильных агентов и запрашивает открытый ключ для дешифрования данных агента MA_{i1}, поиск которого осуществляется по идентификатору агента ID_{MAi1}. После получения открытого ключа и дешифрования данные агента MA_{i1} становятся доступны агентам площадки VBP_k. Управляющий агент UA_k перед вхождением агента MA_{i1} в состав площадки VBP_k предоставляет ему информацию обо всех агентах, функционирующих в ее пределах, тем самым знания агента MA_{i1} о системе пополняются. После возвращения агента MA_{i1} на свой "родной" узел, он генерирует новую пару ключей (ZK_{MAi1}, OK_{MAi1}), а его управляющий агент UA_i обновляет его открытый ключ, хранящийся на сервере безопасности мобильных агентов.

В случае использования системы с децентрализованным управлением безопасностью мобильных агентов (рис. 4) СБМА в открытой мультиагентной виртуальной бизнес-среде 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 аналогичные функции, что и сервер безопасности мобильных агентов: хранит информацию об агентах системы, доступных узлах, виртуальных бизнес-площадках, 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. Рассмотрим принципы взаимодействия основных компонентов ОМАВБС при таком подходе к реализации СБМА (рис. 5).

Пусть некоторый мобильный агент MA_{i1} планирует мигрировать с виртуальной бизнес-площадки VBP_i, расположенной на узле SH_i, на виртуальную бизнес-площадку VBP_k, зарегистрированную на узле SH_k. Агент MA_{i1} отправляет запрос своему управляющему агенту UA_i на разрешение осуществления миграции на VBP_k узла SH_k. Управляющий агент UA_i, получив запрос от агента MA_{i1}, обращается к системе безопасности мобильных агентов агентного представительства узла SH_i, запрашивая информацию для проверки существования узла SH_k и площадки VBP_k соответственно. В случае положительного ответа

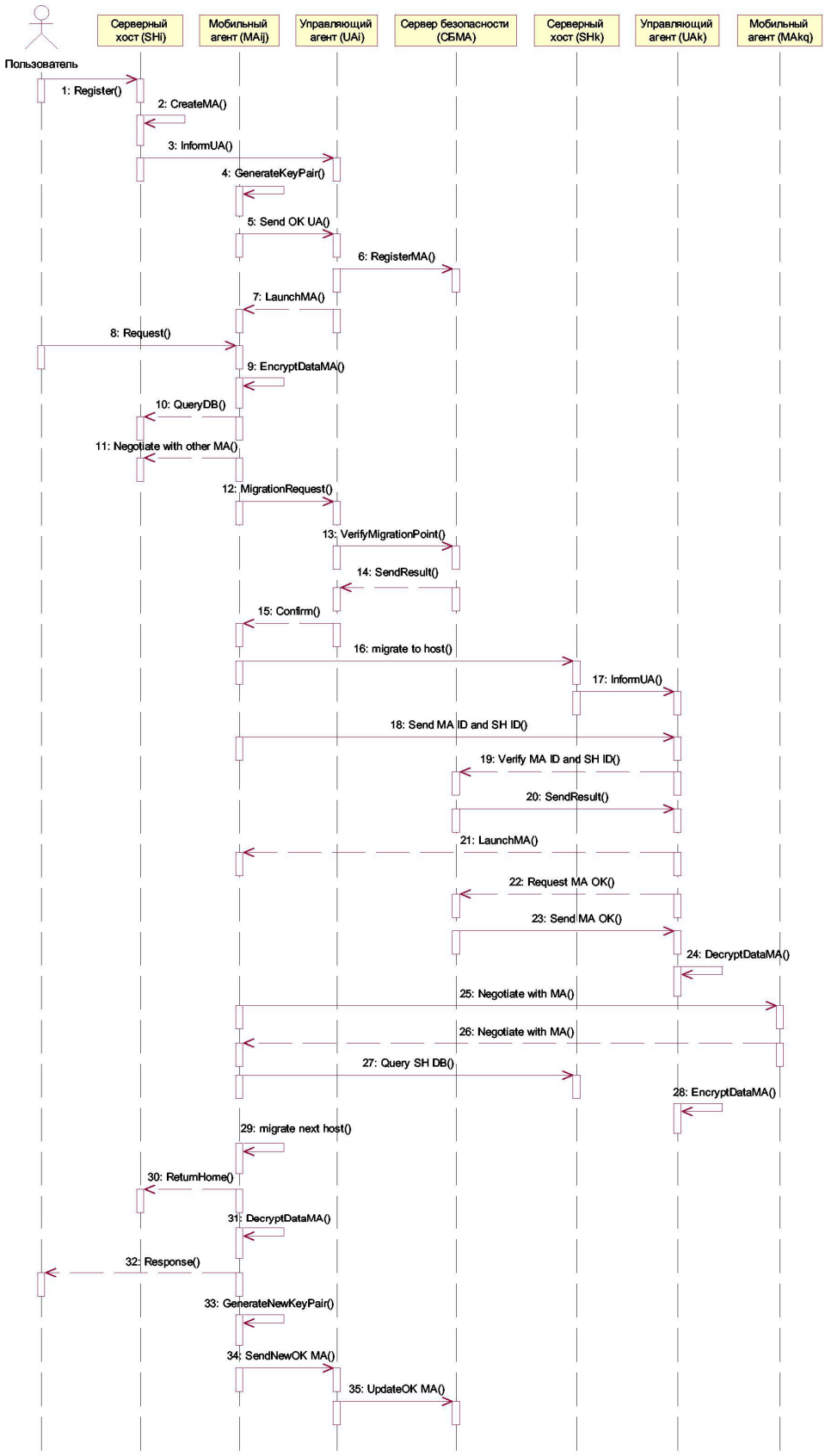

Рис. 3. Диаграмма взаимодействия основных компонентов ОМАВБС с системой централизованного управления безопасностью мобильных агентов

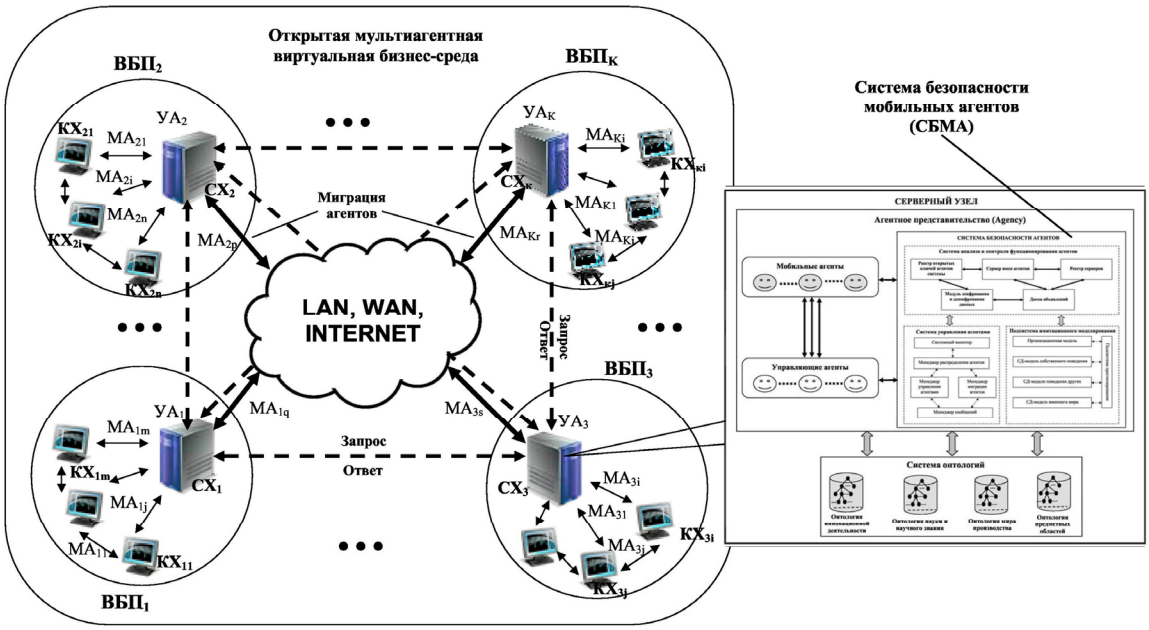

Рис. 4. Открытая мультиагентная виртуальная бизнес-среда с системой децентрализованного управления безопасностью мобильных агентов
(СБМА – система безопасности мобильных агентов; ВБП – виртуальная бизнес-площадка;
МА – мобильный агент; УА – управляющий агент; СХ – серверный хост; КХ – клиентский хост)

управляющий агент UA_i разрешает агенту MA_{il} осуществить миграцию на узел SH_k и инициирует процесс перемещения агента MA_{il} с помощью менеджера миграции агентов. На входе в агентное представительство узла SH_k агент MA_{il} предъявляет управляющему агенту UA_k площадки VBP_k свой уникальный сертификат. Управляющий агент UA_k площадки VBP_k на основе информации, содержащейся в предъявленном сертификате, осуществляет проверку существования в системе узла SH_i и агента MA_{il} в локальном системном реестре и СБМА своего агентного представительства. Если информация подтверждается, то UA_k обращается к удостоверяющему центру, функции которого выполняет управляющий агент UA_i узла SH_i, с которого мигрировал агент MA_{il}, с запросом на подтверждение существования агента MA_{il} и того факта, что ему было разрешено мигрировать на узел SH_k. Если агент UA_i подтверждает факт существования и миграции агента MA_{il} на узел SH_k, управляющий агент UA_k загружает агента MA_{il} в память узла SH_k и предоставляет ему доступ ко всем ресурсам узла SH_k в пределах адресного пространства площадки VBP_k. При этом агент MA_{il} может собирать нужную информацию и вступать в переговоры с агентами, принадлежащими площадке VBP_k.

Если UA_k не получил соответствующих подтверждений о существовании агента MA_{il} в системе или его легальной миграции, агент MA_{il} блокируется, а доступ к ресурсам узла SH_k для него запрещается. Управляющий агент UA_k в этом случае заносит агента MA_{il} в "черный список" и информирует о присутствии "чужого" агента в системе всех известных ему агентов.

Так как все данные D_{MAil}, которыми оперирует агент MA_{il}, зашифрованы закрытым ключом, который неизвестен ни одному из агентов в пределах узла SH_k, управляющий агент UA_k обращается к UA_i и запрашивает открытый ключ для дешифрования данных агента MA_{il}, управляющий агент UA_i предоставляет агенту UA_k открытый ключ агента MA_{il}. После получения открытого ключа и дешифрования данные агента MA_{il} становятся доступны агентам площадки VBP_k. Управляющий агент UA_k перед вхождением агента MA_{il} в состав площадки VBP_k предоставляет ему информацию обо всех агентах, функционирующих в ее пределах, тем самым знания агента MA_{il} о системе пополняются. Вместе с тем, управляющий агент UA_k присваивает агенту MA_{il} специальную метку и заносит информацию о нем в реестр безопасных агентов, тиражируемый в рамках системы. При этом уровень доверия к агенту MA_{il} со стороны других агентов повышается. После возвращения агента MA_{il} на свой "родной" узел, он генерирует новую пару ключей (ZK_{MAil}, OK_{MAil}), а его управляющий агент UA_i обновляет его открытый ключ в СБМА.

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

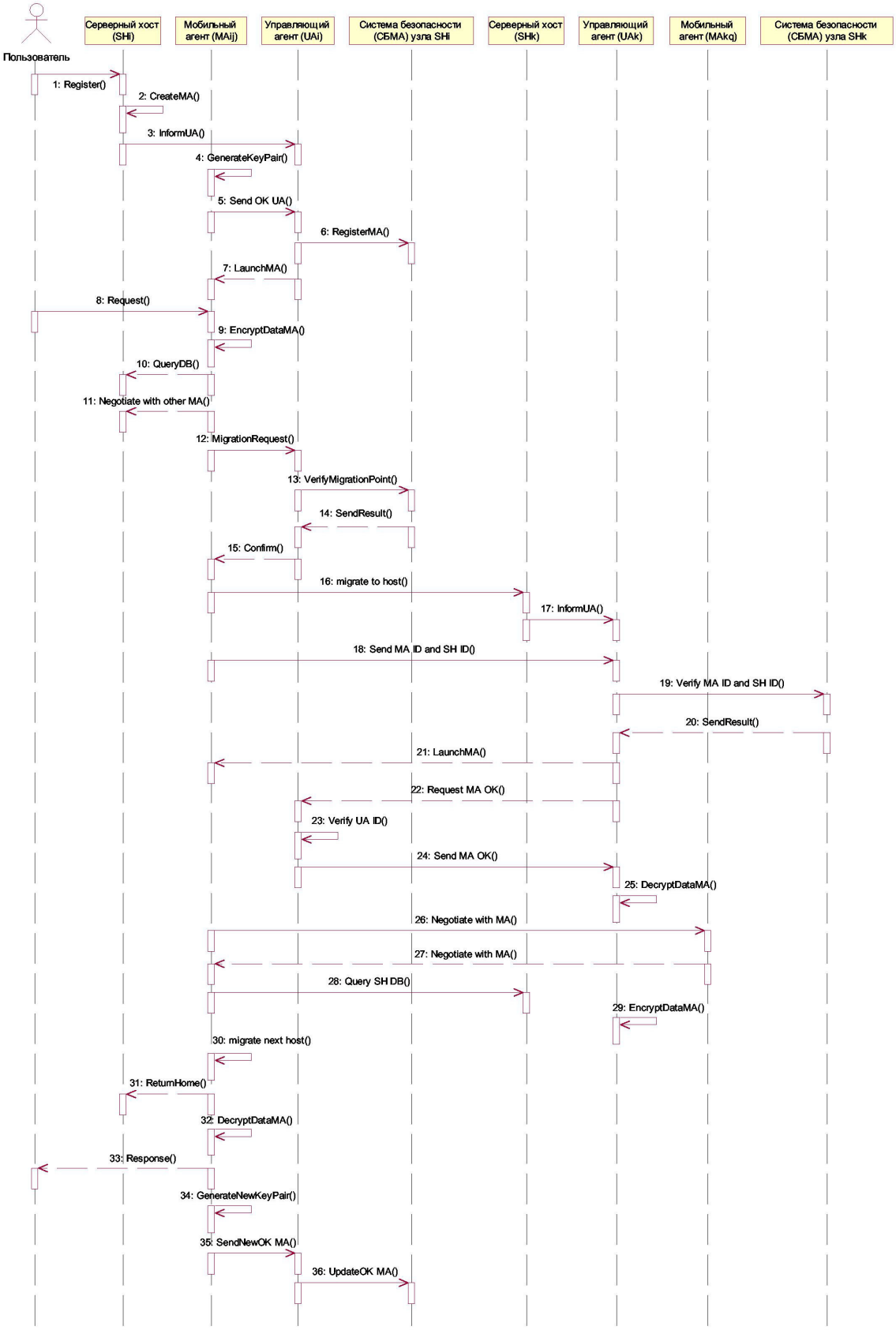

Рис. 5. Диаграмма взаимодействия основных компонентов ОМАВБС с системой децентрализованного управления безопасностью мобильных агентов

Таблица. Параметры вычислительных моделей показателей эффективности функционирования МАС в зависимости от способа реализации СБМА

Параметр	**Описание**
N	Количество серверных узлов в системе
D_{code}	Размер программного кода мобильного агента (МА)
D_{state}	Размер данных, описывающих состояние МА в каждый момент времени, включая информацию о бизнес-предложениях своего владельца, которого он представляет в виртуальной бизнес-среде (за исключение данных, получаемых от других агентов системы в процессе межагентных коммуникаций, либо собираемых в процессе поиска с других узлов системы)
D_{data}	Количество данных, собранных с удаленных серверных и/или клиентских узлов системы
T_{regMA}	Время, необходимое на создание и регистрацию нового агента в системе
$T_{adrListForm}$	Время, необходимое для формирования адресных баз мобильного агента
$T_{genKeyPair}$	Время, необходимое на генерацию пары ключей (ZK_{MA}, OK_{MA})
T_{UAMA}	Время, затрачиваемое на переговоры между МА и его управляющим агентом (УА)
T_{UAUA}	Время, затрачиваемое на переговоры между УА разных виртуальных бизнес-площадок
$T_{updMASS}$	Время, необходимое на обновление информации в СБМА
$T_{verMASH}$	Время, требуемое для проверки существования МА в системе и узла, которого он мигрировал
T_{reqOK}	Время, необходимое на запрос открытого ключа
T_{respOK}	Время, необходимое для получения открытого ключа
R_s	Скорость создания электронной подписи
R_v	Скорость проверки электронной подписи
R_e	Скорость шифрования
R_d	Скорость дешифрования
R_{se}	Скорость поиска информации в базах данных серверных узлов системы / скорость информационного обмена с другими агентами системы
R_{th}	Пропускная способность сети
$T_{reqdata}$	Время, требуемое на запрос данных
D_{init}	Размер МА до его перемещения на удаленный узел системы
T_{init}	Время, требуемое для перемещения МА на удаленный узел системы
D_{mig}	Размер МА в процессе миграции между узлами системы
T_{mig}	Время, затрачиваемое на перемещение МА на удаленный узел, поиск информации и взаимодействие с агентами на удаленном узле
T_{MAth}	Общее время миграции МА между узлами системы
T_{MAAuth}	Время, необходимое на аутентификацию МА в пределах агентного представительства серверного узла
T_{Sdata}	Время, необходимое для создания электронной подписи и шифрования результатов
T_{MAsec}	Время, необходимое для выполнения функций по обеспечению безопасности
T_{MA}, T^{*}_{MA}	Общее время функционирования одного мобильного агента в МАС
T_{MACSCS}	Общее время функционирования МАС, в которой реализованы механизмы централизованного управления безопасностью мобильных агентов
T_{SDTh}	Общее время выполнения мобильного агента поставленной пользователем задачи и представления результатов работы пользователю
C_{AP}	Количество агентных платформ (виртуальных бизнес-площадок), функционирующих в системе
T_{SDAuth}	Время, необходимое для идентификации и аутентификации МА в пределах ВБП
T_{SDSec}	Время, необходимое для выполнения функций по обеспечению безопасности
T_{itnry}	Время, необходимое для формирования маршрута перемещения МА по сети для достижения конкретного узла
T_{MADSCS}	Общее время функционирования МАС, в которой реализованы механизмы децентрализованного управления безопасностью мобильных агентов

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 (архитектура с выделенным сервером), можно отметить основные проблемы систем подобного типа, к которым, согласно работе (*Шишаев*, *Маслобоев*, 2009), можно отнести: 1) уязвимость центрального звена (при отказе сервера безопасности нарушается защита активных компонентов и всей системы в целом, ее безопасность становится под угрозой); 2) высокая нагрузка на центральный сервер управления безопасностью при большом количестве агентов и узлов и, как следствие – ограниченная масштабируемость; 3) централизованное администрирование подразумевает полный контроль над ресурсами на стороне сервера, что не всегда приемлемо, если ресурсы принадлежат разным пользователям.

7. Оценка производительности МАС в зависимости от способа реализации СБМА

Для выбора конкретного варианта реализации СБМА и определения влияния предложенных механизмов управления безопасностью на эффективность функционирования МАС в целом разработаны вычислительные модели показателей эффективности функционирования (производительности) МАС в зависимости от типа реализуемой в ней СБМА – с централизованным или децентрализованным управлением безопасностью. В качестве показателя эффективности функционирования МАС предложено рассматривать общее время работы всех входящих в ее состав мобильных агентов и сервисов безопасности, включающее время, необходимое для успешного решения агентами пользовательских задач, а также время, затрачиваемое на выполнение процедур по обеспечению информационной безопасности агентов и ресурсов системы. Основные параметры вычислительных моделей показателей эффективности функционирования МАС с реализованными механизмами централизованного и децентрализованного управления безопасностью представлены в таблице. Выбор отдельных параметров основан на результатах исследований в области информационной безопасности мобильных агентов в агентно-ориентированных системах электронной коммерции, изложенных в работе (*Kannammal et al.*, 2006).

7.1. Вычислительная модель показателя эффективности функционирования МАС с централизованным управлением безопасностью мобильных агентов

Время, необходимое на создание и регистрацию нового агента в системе:

$$T_{regMA} = T_{MACodeGen} + T_{adrListForm} + T_{genKeyPair} + T_{UAMA} + T_{updMASS},$$

где $T_{MACodeGen}$ – время, требуемое на генерацию программного кода мобильного агента, его запуск и формирование дерева целей агента в зависимости от выбранных пользователем настроек; $T_{adrListForm}$ – время, необходимое для формирования адресных баз мобильного агента; $T_{genKeyPair}$ – время, необходимое на генерацию пары ключей (ZK_{MA}, OK_{MA}) и выдачу агенту сертификата; T_{UAMA} – время, затрачиваемое на переговоры между мобильным агентом и удостоверяющим центром (его управляющим агентом); $T_{updMASS}$ – время, необходимое на обновление информации в СБМА.

В момент создания нового агента в системе его размер определяется размером его программного кода и информацией об его состоянии в текущий момент времени:

$$D_{init} = D_{code} + D_{state},$$

где D_{code} – размер программного кода мобильного агента; D_{state} – размер данных, описывающих состояние МА в каждый момент времени, включая информацию о бизнес-предложениях владельца, которого он представляет в виртуальной бизнес-среде (за исключением данных, получаемых от других агентов системы в процессе межагентных коммуникаций либо собираемых в процессе поиска с других узлов системы).

Когда агент планирует переместиться на некоторый удаленный узел сети, он запрашивает разрешение на осуществление миграции у своего управляющего агента. Время, необходимое на выполнение процесса перемещения агента и проверку существования узла-приемника в системе, куда мигрирует агент, а также шифрования пользовательских запросов и данных определяется как:

$$T_{init} = D_{state} * (1 / R_S) + T_{UAMA},$$

где R_S – скорость создания электронной подписи (или сертификата агента).

В процессе мигрирования между узлами системы агент выполняет задачи, поставленные перед ним пользователем, и по завершении своей работы представляет ему полученные результаты. При этом в процессе сбора, поиска, обработки информации, а также миграции между узлами сети до тех пор, пока

агент не возвратится на свой "родной" узел, где он был сгенерирован, его размер постоянно изменяется и может быть определен следующим образом:

$$D_{mig} = D_{code} + D_{state} + D_{data},$$

где D_{data} – объем данных, собранных с удаленных серверных и/или клиентских узлов системы.

Общее время функционирования одного мобильного агента в системе складывается из времени, которое необходимо ему для взаимодействия с другими агентами системы, анализа, поиска и обработки информации в целях решения поставленной пользователем задачи, а также времени, которое требуется для реализации процедур обеспечения его безопасности, таких как проверка целостности данных и программного кода агента, прохождение процедур аутентификации и идентификации агента в процессе миграции между узлами системы, обеспечение конфиденциальности запросов агента и пользовательских данных, которыми он оперирует.

Допустим T_{mig} – это время, необходимое для перемещения мобильного агента на удаленный узел системы и поиска нужной информации в процессе взаимодействия с другими агентами, функционирующими на данном удаленном узле. Тогда T_{mig} будет рассчитываться по формуле:

$$T_{mig} = (1 / R_{se}) + (D_{mig} / R_{th}),$$

где R_{se} – скорость поиска информации в базах данных серверных узлов системы / скорость информационного обмена с другими агентами системы; R_{th} – пропускная способность сети.

Общее время T_{Math}, затрачиваемое мобильным агентом на выполнение задачи, поставленной пользователем, можно рассчитать по формуле:

$$T_{MAth} = (D_{init} / R_{th}) + T_{init} + (D_{data} / R_{th}) + (N - 1) * T_{mig},$$

где T_{MAth} – общее время миграции МА между узлами системы; N – количество зарегистрированных серверных узлов в системе.

Управляющий агент виртуальной бизнес-площадки удаленного узла, на который мигрировал мобильный агент, инициирует выполнение процедур идентификации и аутентификации мигрировавшего агента, а также осуществляет проверку его существования и узла-отправителя в системе посредством взаимодействия с сервером безопасности мобильных агентов. В случае получения положительного подтверждения, он также запрашивает у СБМА открытый ключ для дешифрования данных мигрировавшего агента. Общее время T_{MAAuth} на выполнение операций, связанных с идентификацией и аутентификацией мобильного агента на удаленном узле и шифрованием/дешифрованием его данных и запросов, может быть вычислено по формуле:

$$T_{MAAuth} = T_{reqdata} + T_{reqOK} + T_{respOK} + (D_{state} * (1 / R_v)),$$

где $T_{reqdata}$ – время, требуемое на запрос данных; T_{reqOK} – время, необходимое на запрос открытого ключа; T_{respOK} – время, необходимое для получения открытого ключа; R_v – скорость проверки электронной подписи (подлинности сертификата агента).

Время T_{Sdata}, затрачиваемое на шифрование и дешифрование запросов и собираемых мобильным агентом данных на удаленном узле в процессе межагентных коммуникаций, можно определить как:

$$T_{Sdata} = D_{data} * ((1 / R_s) + (1 / R_e)),$$

где R_e – скорость шифрования данных.

Время T_{MASec}, необходимое на обеспечение целостности данных и программного кода мобильного агента, а также конфиденциальности информации, которой он оперирует, вычисляется по формуле:

$$T_{MASec} = (D_{data} / R_s) + (D_{data} / R_e) + (D_{data} / R_d) + (D_{data} / R_v) + (N * (D_{state} / R_v)) + (N - 1) * T_{SData},$$

где R_d – скорость дешифрования данных.

Если в процессе выполнения задачи пользователя мобильному агенту необходимо посетить N узлов системы, то ему потребуется осуществить N+1 перемещений (миграций), в рамках каждого из которых будут выполняться процедуры его идентификации и аутентификации с помощью сервисов, предоставляемых СБМА. Тогда, общее время функционирования одного мобильного агента в системе, в которой реализованы механизмы централизованного управления безопасностью, будет определяться следующим образом:

$$T_{MA} = T_{MAth} + (N + 1) * T_{MAAuth} + T_{MASec} + T_{genNewKeyPair} + T_{updMASS}, \quad (1)$$

где T_{MAAuth} – время, необходимо на аутентификацию МА в пределах агентного представительства серверного узла; T_{MASec} – время, необходимое для выполнения функций по обеспечению безопасности; $T_{genNewKeyPai}$ – время, необходимое на генерацию новой пары ключей (ZK_{MA}, OK_{MA}) или создание нового сертификата, после возвращения мобильного агента на "родной" узел.

Следовательно, если в системе зарегистрировано M мобильных агентов, то общее время функционирования такой МАС, в которой реализуется централизованная СБМА:

$$T_{MACSCS} = \sum^{M}_{i=1} T_{MAi}. \quad (2)$$

Под общим временем функционирования МАС в данном случае понимается количество времени, которое необходимо для успешного выполнения всех поставленных перед агентами задач (суммарное время функционирования агентов системы), включая время на обработку распределенных данных, выполнение процедур идентификации и аутентификации, миграцию между узлами сети, межагентные коммуникации и т.д. Учитывая тот факт, что рассматриваемые в работе МАС являются открытыми, распределенными и самоорганизующимися, то данный показатель времени может быть рассчитан лишь для конкретного периода эксплуатации МАС в зависимости с учетом сложности поставленных перед агентами задач.

Таким образом, характеристикой производительности МАС является время T_{MACSCS}, которое необходимо для успешного выполнения процедур обеспечения целостности данных и программного кода мобильных агентов (шифрование и дешифрование информации), реализации методов аутентификации и идентификации агентов в системе, а также для решения пользовательских задач.

Производительность МАС с СБМА с централизованным управлением безопасностью в основном зависит от пропускной способности канала связи между сервером безопасности мобильных агентов и узлами сети, на которых функционируют управляющие агенты. Как видно из формул (1) и (2), при увеличении количества подключаемых к системе узлов и мобильных агентов значительно увеличивается нагрузка на центральный сервер безопасности мобильных агентов, тем самым уменьшается производительность МАС. Повышения эффективности функционирования централизованной СБМА можно достичь за счет повышения скорости шифрования и дешифрования данных агентов, которая в основном зависит от разновидности используемых криптографических алгоритмов и/или длины генерируемых секретных ключей, а также за счет увеличения скорости установки и проверки электронной подписи.

7.2. Вычислительная модель показателя эффективности функционирования МАС с децентрализованным управлением безопасностью мобильных агентов

При реализации механизмов децентрализованного управления безопасностью и соответствующей СБМА в МАС отсутствует единый центр управления безопасностью. В этом случае все функции по обеспечению информационной безопасности агентов и данных, которыми они оперируют в системе, распределяются между управляющими агентами, функционирующими на серверных узлах системы, а СБМА реализуется в пределах каждого из агентных представительств, зарегистрированных на серверных узлах системы. Реализация такого подхода к обеспечению безопасности позволяет распределить нагрузку по выполнению процедур идентификации и аутентификации агентов системы, проверки целостности программного кода и данных агентов, шифрования и дешифрования данных между виртуальными бизнес-площадками, тем самым сократить нагрузку на коммуникационную инфраструктуру.

Производительность МАС с децентрализованной СБМА зависит не только от количества агентов, мигрирующих между узлами сети, но также и от количества виртуальных бизнес-площадок, функционирующих в системе. Общее время работы мобильного агента в МАС, как уже отмечалось выше, складывается в основном из времени, затрачиваемого агентом на поиск и обработку необходимой информации (поиск в базах данных серверных узлов, информационный обмен с другими агентами системы и т.д.), и времени, затрачиваемого на прохождение агентом контрольных процедур идентификации и аутентификации, проверки конфиденциальности и целостности кода и данных агента, шифрования / дешифрования данных агента при перемещении между виртуальными бизнес-площадками системы.

Таким образом, общее время работы мобильного агента до завершения выполнения поставленной перед ним пользователем задачи T_{SDTh} можно рассчитать по формуле:

$$T_{SDTh} <= T_{MAth} + (C_{AP} * (D_{mig} / R_{th})),$$

где C_{AP} – количество агентных платформ (виртуальных площадок), функционирующих в системе.

Время, необходимое для выполнения процедур идентификации и аутентификации мобильного агента в пределах виртуальных бизнес-площадок, на которые мигрирует агент:

$$T_{SDAuth} = C_{AP} * T_{MAAuth}.$$

Время T_{SDSec}, затрачиваемое на выполнение процедур проверки и обеспечения целостности и конфиденциальности программного кода и данных мобильного агента, определяется как:

$$T_{SDSec} <= T_{MASec} + (C_{AP} * ((D_{code} / R_{v}) + T_{SData})),$$

где T_{SData} – время, необходимое для создания создание электронной подписи и шифрования результатов.

В итоге, общее время T^*_{MA} работы мобильного агента в МАС с децентрализованной СБМА включает: время, затрачиваемое агентом на поиск и обработку данных в процессе межагентных коммуникаций, время на выполнение процедур идентификации и аутентификации агента, время, необходимое на формирование маршрута движения по сети, заполнения адресных баз агента и реализации процедур перемещения агента на нужный узел или виртуальную бизнес-площадку, время на проверку и обеспечение целостности и конфиденциальности программного кода и данных агента, время на переговоры с управляющими агентами системы. Тогда T^*_{MA} можно вычислить следующим образом:

$$T^*_{MA} <= T_{SDTh} + T_{SDAuth} + C_{AP} * T_{itnry} + T_{SDSec} + T_{genNewKeyPair} + T_{updMASS}, \quad (3)$$

где T_{itnry} – время, необходимое для формирования маршрута перемещения МА по сети для достижения конкретного узла.

Таким образом, если в системе присутствует M мобильных агентов, то общее время функционирования МАС с децентрализованной СБМА:

$$T_{MADSCS} <= \sum^{M}_{i=1} T^*_{MAi}. \quad (4)$$

Учитывая, что СБМА с децентрализованным управлением безопасностью должна обеспечивать наибольшую производительность МАС, по сравнению с СБМА с централизованным управлением безопасностью, то, следовательно, должно выполняться следующее неравенство:

$$T_{MADSCS} <= T_{MACSCS}. \quad (5)$$

Преобразовав левую и правую часть выражения (5) с учетом выражений (1-4) и выполнив необходимые сокращения, получим:

$$T_{SDTh} + T_{SDAuth} + C_{AP} * T_{itnry} + T_{SDSec} <= T_{MAth} + (N + 1) * T_{MAAuth} + T_{MASec}.$$

С ростом числа виртуальных бизнес-площадок и подключаемых к системе узлов и агентов увеличивается интенсивность межагентных коммуникаций и число миграций агентов между узлами сети. При реализации СБМА с централизованным управлением безопасностью нагрузка на центральный сервер безопасности в этом случае значительно возрастает и, соответственно, увеличивается общее время работы агентов по выполнению пользовательских задач. При этом эффективность функционирования МАС в целом снижается. В случае же реализации СБМА с децентрализованным управлением безопасностью вся нагрузка по выполнению функций безопасности распределяется между управляющими агентами виртуальных бизнес-площадок и агентными представительствами серверных узлов системы. Вместе с тем, агентные представительства серверных узлов, помимо процедур безопасности (идентификация и аутентификация агентов системы, шифрование и дешифрование данных агентов), обеспечивают выполнение процедур формирования маршрутов дальнейших перемещений мобильных агентов по сети в зависимости от поставленной цели, а также проверку целостности и конфиденциальности программного кода и данных агентов. В результате, децентрализованное управление безопасностью, в независимости от увеличения количества подключаемых к системе новых узлов или агентов, обеспечивает балансирование нагрузки по обеспечению безопасности между серверными узлами системы, гибкость и эффективность процесса идентификации и аутентификации агентов, а также сокращает общее время на его выполнение, что, в свою очередь, приводит к повышению производительности МАС. В связи с этим можно предположить, что показатель T_{MADSCS} лучше, чем T_{MACSCS}. Это позволяет сделать выбор в пользу СБМА с механизмами децентрализованного управления безопасностью при практических реализациях открытых распределенных проблемно-ориентированных МАС, ориентированных на использование в различных предметных областях.

8. Практическая реализация

Активные компоненты открытой мультиагентной виртуальной бизнес-среды (агенты) и предложенные механизмы управления информационной безопасностью реализованы в программной инструментальной среде разработки агентов и мультиагентных систем JADE (Java Agent Application Environment) (*Balachandran, Enkhsaikhan*, 2007), поддерживающей стандарты FIPA и MASIF и ориентированной на создания распределенных приложений на платформе Java, включая возможность реализации мобильных агентов, способных мигрировать между узлами сети. Для поддержания эффективного информационного обмена и обеспечения единых стандартов диалога между агентами системы используется специальный язык FIPA’s Agent Communication Language (ACL) (*O'Brien, Nicol*, 1998). Механизм переговоров между агентами системы основан не только на использовании общего языка коммуникации, но и на общей онтологии предметной области. Функции онтологии выполняет

концептуальная модель виртуальной бизнес-среды (*Маслобоев и др.*, 2007), являющейся частью ментальной подсистемы гибридной InteRRap-архитектуры агента с имитационным аппаратом (*Маслобоев*, 2009а). Она определяет цели и правила взаимодействия агентов, а также отношения между ними.

9. Заключение

В работе проанализированы основные проблемы и виды угроз информационной безопасности открытых проблемно-ориентированных распределенных мультиагентных информационных систем. Рассмотрены современные подходы, ориентированные на решение задач, связанных с обеспечением информационной безопасности агентов и мультиагентных систем.

В ходе проведенных исследований были получены следующие основные результаты:

1) Предложены подходы к обеспечению информационной безопасности в OMAC, основанные на реализации механизмов централизованного и децентрализованного управления безопасностью мобильных агентов, а также имитационном моделировании поведения их активных программных компонентов. Разработанные механизмы управления безопасностью составляют основу подсистемы информационной безопасности, реализованной в виде комплекса программ в рамках системы информационной поддержки инновационной деятельности (*Маслобоев, Шишаев*, 2009), представляющей собой открытую мультиагентную виртуальную бизнес-среду инноваций.

2) Разработан метод формирования комплексной самоорганизующейся системы децентрализованного управления безопасностью мобильных агентов в OMAC, реализующей механизмы аутентификации агентов с помощью открытых ключей посредством удостоверяющих центров. Метод ориентирован на открытые сети агентов и обеспечивает на основе реализации механизмов самоорганизации агентов (формирование в рамках OMAC виртуальных площадок, объединяющих агентов с близкими целями в коалиции – частные сети агентов по интересам) автоматическое формирование удостоверяющих центров (центров сертификации), образующих систему безопасности мобильных агентов в OMAC, представляющую собой самоорганизующуюся инфраструктуру открытых ключей PKI с децентрализованной архитектурой. Децентрализованный характер функционирования самоорганизующейся системы безопасности мобильных агентов на основе сертификатов за счет распределения функций по управлению безопасностью между управляющими агентами (удостоверяющими центрами) обеспечивает балансирование нагрузки на инфраструктуру безопасности OMAC, тем самым повышая производительность OMAC в целом.

3) Выполнен сравнительный анализ предложенных систем безопасности мобильных агентов в зависимости от типа управления безопасностью – централизованное или децентрализованное управление безопасностью агентов в OMAC. Результаты анализа подтверждают целесообразность выбора и реализации в рамках OMAC механизмов децентрализованного управления безопасностью мобильных агентов.

4) Предложена методика и вычислительные модели критериев оценки эффективности (производительности) систем безопасности мобильных агентов с реализованными механизмами централизованного и децентрализованного управления безопасностью.

Полученные результаты могут найти широкое применение при решении практических задач, связанных с анализом рисков информационной безопасности конкретных объектов информатизации и разработкой новых методов и технологий их снижения.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект № 08-07-00301-а "Разработка информационной технологии и распределенной информационно-аналитической среды поддержки инновационной деятельности").

Литература

Balachandran B.M., Enkhsaikhan M. Developing multi-agent e-commerce applications with JADE. *Proceedings of the 11th International conference, KES 2007 and XVII Italian workshop on neural networks conference on Knowledge-based intelligent information and engineering systems*, Part III, *Springer-Verlag Berlin, Heidelberg*, p.941-949, 2007.

Cao Y., Fu Ch. An efficient implementation of RSA digital signature algorithm. *Proceedings of the 2008 International Conference on Intelligent Computation Technology and Automation (ICICTA'2008), IEEE Computer Society Washington, DC, USA*, v.2, p.100-103, 2008.

Kannammal A., Iyengar N.Ch.S.N. A model for mobile agent security in e-business applications. *International Journal of Business and Information*, v.2, N 2, p.185-197, 2007.

Kannammal A., Ramachandran V., Iyengar N.Ch.S.N. Secure MobileAgent system for e-business applications. *Proceedings of 4th ACS/IEEE International Conference on Computer Systems and Applications*, *Dubai/Sharjah, UAE*, p.326-329, 2006.

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*, N 23(4), p.199-212, 2004.

Neeran K.M., Tripathi A.R. Security in the Ajanta MobileAgent system. *Technical Report. Department of Computer Science, University of Minnesota*, May 1999.

O'Brien P.D., Nicol R.C. FIPA – towards a standard for software agents. *BT Technology Journal, Kluwer Academic Publishers Hingham, MA, USA*, v.16, Iss. 3 (July 1998), p.51-59, 1998.

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*, v.54, 2004.

Peng J., Wu Q. Research and Implementation of RSA Algorithm in Java. *Proceedings of the 2008 International Conference on Management of e-Commerce and e-Government (ICMECG'2008)*, IEEE *Computer Society Washington, DC, USA*, p.359-363, 2008.

Ramchurn S.D., Huynh D., Jennings N.R. Trust in multi-agent systems. *The Knowledge Engineering Review. Cambridge University Press New York, NY, USA*, v.19, Iss. 1 (March 2004), p.1-25, 2004.

Sander T., Tschudin Ch.F. Protecting MobileAgents against malicious hosts. *In Giovanni Vigna (ed.), MobileAgents and Security, LNCS, Springer*, p.44-60, 1998.

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*, v.2, p.1165-1166, 2000.

Городецкий В.И., Котенко И.В., Юсупов Р.М. Защита компьютерных сетей. *Вестник РАН, М., Наука*, № 7, с.668-670, 2006.

Котенко И.В. Интеллектуальные механизмы управления кибербезопасностью. *Управление рисками и безопасностью: Труды Института системного анализа РАН, М., УРСС*, т.41, с.74-103, 2009.

Котенко И.В., Уланов А.В. Многоагентное моделирование механизмов защиты от распределенных компьютерных атак. *Информационные технологии*, № 2, с.38-44, 2009.

Маслобоев А.В. Гибридная архитектура интеллектуального агента с имитационным аппаратом. *Вестник МГТУ: Труды Мурманского государственного технического университета*, т.12, № 1, с.113-125, 2009a.

Маслобоев А.В. Мультиагентная технология формирования виртуальных бизнес-площадок в едином информационно-коммуникационном пространстве развития инноваций. *Научно-технический вестник СПбГУ ИТМО*, № 6(64), с.83-89, 2009b.

Маслобоев А.В. Самоорганизация программных агентов в распределенной мультиагентной системе информационной поддержки инноваций. *Теория и практика системной динамики: Труды III Всерос. науч. конф. Апатиты, КНЦ РАН*, с.103-114, 2009c.

Маслобоев А.В., Путилов В.А., Шишаев М.Г. Концептуальная модель агентно-ориентированной виртуальной бизнес-среды развития инноваций. *Информационные технологии в региональном развитии: Сб. науч. тр. ИИММ КНЦ РАН, Апатиты, КНЦ РАН*, вып. VII, с.15-27, 2007.

Маслобоев А.В., Шишаев М.Г. Одноранговая распределенная мультиагентная система информационно-аналитической поддержки инновационной деятельности. *Научно-технический вестник СПбГУ ИТМО*, № 4(62), с.108-114, 2009.

Полянская О.Ю., Горбатов В.С. Инфраструктура открытых ключей. Учебное пособие. *М., Изд-во: Интернет-университет информационных технологий, Лаборатория Знаний*, 368 с., 2007.

Путилов В.А., Шишаев М.Г., Олейник А.Г. Технологии распределенных систем информационной поддержки инновационного развития региона. *Труды Института системного анализа РАН, М., УРСС*, т.39, с.40-64, 2008.

Рыбина Г.В., Паронджанов С.С. Модели, методы и программные средства поддержки взаимодействия интеллектуальных агентов. *Информационные технологии и вычислительные системы, М., УРСС*, вып. 3, с.22-29, 2008.

Тарасов В.Б. От многоагентных систем к интеллектуальным организациям: философия, психология, информатика. *М., Едиториал УРСС*, 352 с., 2002.

Федоров А.М., Датьев И.О. Проблемы информационной безопасности систем информационно-аналитической поддержки управления сложными объектами. *Прикладные проблемы управления макросистемами: Мат. докл. VII Всерос. конф. (Апатиты, 31 марта – 4 апреля 2008 г.). Апатиты, КНЦ РАН*, с.44-45, 2008.

Шишаев М.Г., Маслобоев А.В. Архитектура и современные технологии информационных систем поддержки развития открытых инноваций. *Инновации*, №8(142), с.2-8, 2009.