УДК 004.891.2

В.И. Васильев, Н.В. Белков

ОРГАНИЗАЦИОННЫЙ ПОДХОД К ПРОЕКТИРОВАНИЮ МУЛЬТИАГЕНТНОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В настоящее время актуальной является проблема защиты персональных данных при их обработке в информационных системах. Целью исследования является проектирование мультиагентной системы поддержки принятия решений по защите персональных данных. Предлагается организационный подход к проектированию на основе методологии O-MASE, доработанной включением в процесс проектирования этапа построения онтологий. Дается описание применения подхода к созданию целевой системы поддержки принятия решений. Статья содержит 3 рисунка и 9 библиографических источников.

Персональные данные; мультиагентные системы; системы поддержки принятия решений; онтологии; информационная безопасность.

V.I. Vasilyev, N.V. Belkov

ORGANIZATIONAL APPROACH TO THE DESIGN OF MULTIAGENT DECISION SUPPORT SYSTEM FOR PERSONAL DATA PROTECTION

The problem of personal data protection during its processing in information systems is relevant today. Purpose of the research is to design multiagent decision support system for personal data protection. Organization approach to the design based on the O-MASE methodology is offered. That methodology is refined by adding ontology creation stage to the design process. Approach application to the target decision support system engineering is described. Paper consist of 3 figures and 9 references.

Personal data; multiagent systems; decision support systems; ontologies; information security.

Введение. Активная деятельность по защите персональных данных и исследования связанных с нею вопросов в нашей стране начались после ратификации Конвенции Совета Европы «О защите личности в связи с автоматической обработкой персональных данных», принятия в июле 2006 г. Федерального закона «О персональных данных» и выхода ряда подзаконных нормативных актов. При выполнении требований российского законодательства операторы персональных данных и специалисты по защите информации столкнулись с большим количеством проблем [2]. Несмотря на то, что многие организации, занимающиеся защитой информации, разработали методики обеспечения безопасности персональных данных: обследования информационных систем и построения системы защиты, в данной области имеется ряд существенных проблем и нерешенных вопросов.

Прежде всего, организации, привлекающие к работам третьих лиц, не имеют возможности проверить необходимость предлагаемых мероприятий по защите и оценить эффективность принимаемых решений. Привлекаемые предприятия стремятся продать и внедрить как можно большее количество средств защиты, умышленно игнорируя при этом уже принятые меры безопасности. Подобная избыточность увеличивает затраты на создание системы защиты.

Еще одним открытым вопросом остается оценка эффективности принятых решений и анализ рисков. В настоящее время отсутствует какая-либо методика оценки рисков и применимости требований по защите персональных данных, учитывающая особенности предметной области. Единственной предлагаемой нормативными документами оценкой является достаточно грубое определение актуальности угроз.

Одной из наиболее значимых проблем является отсутствие на предприятиях системы менеджмента информационной безопасности персональных данных. Сложившаяся в настоящее время практика заключается в том, что все действия по обеспечению безопасности персональных данных выполняются в формате разового мероприятия. Эксплуатация же системы защиты осуществляется без каких-либо дальнейших модификаций. При этом очевидно, что процесс обеспечения безопасности информации, а особенно персональных данных, должен быть непрерывным.

На основе анализа перечисленных проблем можно сделать вывод, что актуальной является задача создания системы поддержки принятия решений (СППР) по защите персональных данных, выполняющей следующие ключевые функции:

1. Формирование подробного описания информационных систем персональных данных, их выделение и классификация.
2. Автоматизированное формирование моделей угроз и моделей злоумышленника.
3. Выбор наилучшего варианта построения системы защиты персональных данных.
4. Априорная оценка эффективности применяемых мер по защите персональных данных, анализ рисков.
5. Управление (менеджмент) информационной безопасностью персональных данных.

При создании системы защиты персональных данных и управлении информационной безопасностью на предприятии необходимо задействовать сотрудников различного рода деятельности: управленцев, администраторов вычислительной сети, администраторов информационных систем, специалистов по информационной безопасности, руководителей подразделений. При этом достаточно велико число вовлекаемых в процесс участников, каждый из которых принимает специфические решения на основе собственной системы знаний, используя при этом информацию, полученную от других участников процесса. В таких случаях одним из наиболее эффективных подходов является применение технологий распределенного искусственного интеллекта, основным направлением развития которого являются мультиагентные системы (МАС).

1. Анализ подходов к проектированию мультиагентных систем. В области информационной безопасности мультиагентные системы чаще всего используются при организации защиты распределенных вычислительных сетей и построении распределенных систем обнаружения атак [1, 4]. Проводились некоторые исследования по обеспечению поддержки принятия решений по защите информации [3]. Тем не менее предложенные системы поддержки принятия решений не учитывают особенностей персональных данных, как самостоятельной категории конфиденциальной информации.

Применение классического объектно-ориентированного подхода к проектированию мультиагентных систем оказывается очень трудоемким, поскольку строение и поведение агентов сложнее, чем объектов. Для эффективного построения сложных МАС необходима методология, описывающая полный процесс проектирования от высокоуровневых моделей до программной реализации. Подобные методологии начали разрабатываться в начале 2000 гг. Наиболее известными и широко распространенными методами в настоящее время являются: Gaia, Tropos, MASE, O-MASE [5, 9]. Однако все перечисленные подходы имеют недостатки, ограничивающие возможность их применения.

Так, наиболее существенными недостатками методологий Gaia и MASE являются: отсутствие процессов моделирования предметной области, статичность организационной структуры и отсутствие этапов низкоуровневого проектирования, что затрудняет их применение на практике. Методология Tropos неоднозначна, в ней не определена четкая последовательность переходов между этапами, что не

позволяет проследить корректность всех выполняемых действий, а также задать взаимосвязь между системой и окружающей средой. В конечном итоге, Tropos оказывается применимой только для небольших и достаточно простых МАС.

Наибольшей проработанностью и законченностью отличается методология O-MASE (Organization-based Multiagent System Engineering Process Framework). Данная методология разработана сотрудниками Канзасского государственного университета (США) на основе методологии MASE. Проанализировав недостатки предыдущей методологии, разработчики предложили подход, который рассматривает МАС не как простую совокупность агентов, а как организацию, которая активно взаимодействует с окружающей средой и имеет внутреннюю политику, регулирующую деятельность агентов. Кроме того, был разработан программный продукт agentTools3, автоматизирующий многие этапы проектирования. Тем не менее в O-MASE для моделирования предметной области и политик используются достаточно примитивные модели, а поддержка онтологий не предусмотрена.

В настоящей статье предложен организационный поход к проектированию мультиагентных систем, в основе которого лежит методология O-MASE, доработанная таким образом, что в процесс проектирования включается этап формирования онтологий.

2. Этапы проектирования системы мультиагентной СППР по защите персональных данных. Одним из основных преимуществ организационного подхода, основанного на методологии O-MASE, является то, что он не определяет какой-либо фиксированной последовательности этапов. Вместо этого разработчику системы предоставляются рекомендации по составлению собственного метода проектирования [6], представленные в табл. 1. Используя данные рекомендации, проектировщик самостоятельно организует свою деятельность, определяя перечень необходимых этапов и их последовательность на основе требований, предъявляемых к мультиагентной системе.

При формировании общих требований к СППР было принято решение, что агенты будут представлять определенные должностные лица в организации. Таким образом, все значительные изменения в структуре системы агентов, так или иначе, будут инициироваться пользователями. В этом случае от системы не требуется автономная адаптация к изменениям окружающей среды. Как отмечают разработчики методологии [7, 8], при разработке подобных систем нет необходимости в формализации индивидуальных возможностей агентов и ролей. По этой причине из процесса проектирования СППР исключаются этапы, связанные с описанием возможностей. Это такие этапы как *Моделирование возможностей* и *Моделирование операций*.

Таблица 1

Рекомендации по формированию метода

Задача	Результат
Описание требований	Спецификация требований
Моделирование целей	Модель целей
Уточнение целей	Уточненная модель целей
Моделирование предметной области	Модель предметной области
Моделирование организационных интерфейсов	Организационная модель
Моделирование ролей	Ролевая модель
Детализация ролей	Описание ролей
Моделирование классов агентов	Модель классов агентов
Моделирование протоколов	Модель протоколов
Моделирование политик	Модель политики
Моделирование планов действий	Модель плана действий
Моделирование возможностей	Модель возможностей
Моделирование операций	Модель операций
Генерация программного кода	Код программы

Также из процесса проектирования исключаются этапы *Детализация ролей* и *Моделирование политик*. Документ, создаваемый на этапе детализации ролей, дублирует сведения, отображаемые на диаграмме ролей, поэтому соответствующий этап может быть опущен при достаточно подробном описании ролей на диаграмме. Во время моделирования политик задаются правила, описывающие требуемое поведение проектируемой системы. При разработке СППР по защите персональных данных все необходимые требования и ограничения будут определены в наборе онтологий. Онтологии также содержат подробное описание предметной области, что позволяет заменить этапом *Построение онтологий* не только фазу *Моделирование политик*, но и *Моделирование предметной области.* В конечном виде метод проектирования мультиагентной СППР по защите персональных данных состоит из 9 этапов:

Этап 1. Описание требований.
Этап 2. Построение онтологий.
Этап 3. Моделирование целей.
Этап 4. Уточнение целей.
Этап 5. Моделирование организационных интерфейсов.
Этап 6. Моделирование ролей.
Этап 7. Моделирование классов агентов.
Этап 8. Моделирование протоколов.
Этап 9. Моделирование планов действий.
Этап 10. Генерация программного кода.

На этапах 3–10 работа осуществляется в среде *agentTool3*.

3. Описание требований к СППР. Формирование требований к конечному продукту является первоначальным этапом любого процесса проектирования. Ключевые функции системы поддержки принятия решений по защите персональных данных представлены во введении. Разрабатываемая система должна обеспечивать информационную поддержку не только во время создания, но и в течение всего жизненного цикла системы защиты персональных данных. Условия и процессы обработки персональных данных в организации могут значительно изменяться. При этом СППР должна иметь возможность отследить произошедшие изменения, распознать их и выбрать соответствующие реакции. В противном случае эффективность, принимаемых мер по защите персональных данных, значительно снижается или стремится к нулю.

Для определения спецификации требований к системе предлагается использовать циклическую модель Деминга, которая активно применяется при проектировании развивающихся во времени информационных систем и закреплена в ряде международных стандартов информационной безопасности, таких как ИСО/МЭК 27001 и ИСО/МЭК ТО 18044. Модель Деминга реализует цикл «Планирование (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (PCDA), на каждом из этапов которого определяются требования к СППР.

Планирование:

1. Ввод, систематизация и хранение необходимой информации об организации, ее организационной структуре и процессах обработки персональных данных, средствах вычислительной техники, информационных системах и принятых мерах по защите информации.
2. Выделение и классификация информационных систем персональных данных (ИСПДн).

Осуществление:

1. Построение моделей угроз и моделей злоумышленника (потенциального нарушителя).
2. Выбор возможных средств защиты и формирование вариантов построения системы защиты персональных данных (СЗПДн).

3. Априорная оценка эффективности различных вариантов построения СЗПДн. Анализ рисков.
4. Выбор наилучшего варианта построения системы защиты.

Проверка:

1. Оценка эффективности принятых мер защиты и текущего уровня защищенности.
2. Мониторинг вносимых изменений.
3. Анализ изменений. Выбор действий реагирования на изменения.

Действие:

1. Выполнение действий реагирования на изменения:
   - изменение структуры и свойств ИСПДн;
   - изменение класса ИСПДн;
   - разработка/доработка моделей угроз и злоумышленника;
   - изменение состава СЗПДн.

К этапу описания требований, как и к любому другому этапу метода, можно вернуться в любое время для уточнения и дополнения.

4. Построение онтологий. Онтология представляет собой форму представления знаний, отражающую ключевые термины предметной области, их свойства, а также взаимоотношения между терминами. Кроме того, в онтологии можно включать аксиомы, отражающие семантику происходящих в предметной области процессов, описывающие ограничения и условия. В последние годы онтологии стали широко использоваться в сложных, распределенных информационных системах, работающих со знаниями. Выбор онтологического подхода к формированию модели знаний предметной области и моделей знаний отдельных агентов обусловлен рядом преимуществ онтологий:

1. Онтологии обеспечивают разделяемый словарь, используемый агентами при взаимодействии и гарантирующий, что сообщение, посланное одним агентом, будет однозначно понято другими агентами. Термины из онтологии и их свойства используются в качестве параметров протоколов межагентного взаимодействия. При наличии инструментов сравнения и отображения онтологий может быть обеспечено взаимодействие мультиагентной системы со сторонними информационными системами, использующими иные онтологии.
2. На основе онтологий могут быть реализованы механизмы принятия решений при помощи продукционных правил. Средства работы с онтологиями имеют собственные «решатели», позволяющие получать новые знания из имеющихся. При этом уменьшается сложность отдельных интеллектуальных агентов, поскольку не требуется использование отдельных механизмов логического вывода.
3. Использование онтологий позволяет повысить гибкость системы и возможность повторного ее использования. Путем внесения изменений в используемые агентами онтологии можно изменить логику их работы. При этом не требуется вносить изменений в программный код.
4. Онтологии позволяют организовать человеко-машинный интерфейс.

В мультиагентной системе поддержки принятия решений по защите персональных данных используется два вида онтологий, образующих трехуровневую иерархию. На верхнем уровне располагается мета-онтология. Данная онтология определяет ключевые понятия из области мультиагентных систем. За основу мета-онтологии принята мета-модель методологии O-MASE, доработанная с учетом особенностей разрабатываемой системы. В нее входят такие понятия как: агент, роль, цель, протокол, сообщение и др.

На следующих двух уровнях располагаются онтологии предметной области защиты персональных данных. Второй уровень занимает общая онтология предметной области, отображающая основные понятия и взаимоотношения между ними, а также общие условия функционирования СППР и ограничения, накладываемые на систему в целом. Данная онтология может использоваться для организации взаимодействия со сторонними информационными системами. На нижнем уровне располагаются онтологии классов агентов, которые отображают модели знаний отдельных агентов. Они получаются путем детализации общей онтологии, добавлением понятий и отношений, используемых исключительно заданным классом агентов, а также исключением из общей онтологии понятий, не нужных агенту во время работы. Использование двухуровневой системы онтологий предметной области позволяет повысить гибкость системы в целом и упростить отдельные агенты.

Методологией O-MASE не предусмотрено использование онтологий. Вместо них имеются собственные инструменты для создания моделей предметной области и моделей политик. Соответственно методология не содержит описания методов создания онтологий. Формирование онтологий предметной области защиты персональных данных осуществляется следующим образом.

Первоначально формируется словарь терминов предметной области. В качестве источников знаний для словаря использовались: нормативно-методическая документация по персональным данным, проектно-техническая документация на разработанные ранее системы защиты персональных данных, эксперты в области информационной безопасности. Для извлечения знаний из документации использовались средства лингвистического анализа. Получение знаний от экспертов осуществлялось путем анкетирования. На основе словаря сроится тезаурус путем формирования иерархии терминов и определения отношений между ними. Наконец, тезаурус дополняется функциями интерпретации (аксиомами), после чего он становится онтологией.

Для построения онтологий использовался язык OWL (Ontology Web Language) и онтологический редактор Protege. Описание продукционных правил осуществлялось на языке SWRL (Semantic Web Rule Language).

5. Моделирование целей. Целью моделирования ролей является преобразование исходных требований к системе в совокупность структурированных целей, достигаемых системой. Построение модели целей является одним из начальных этапов большинства подходов к проектированию мультиагентных систем. Модель целей в методологи O-MASE представляет собой дерево целей, связанных между собой отношениями И/ИЛИ [8]. Главная цель раскладывается на несколько подцелей. Если для достижения главной цели требуется выполнение всех подцелей, то они связываются отношениями **И**. Если же достаточно выполнения хотя бы одной из подцелей, то они соответственно связываются с главной целью отношениями **ИЛИ**. Так продолжается до тех пор, пока не будет достигнут требуемый уровень детализации.

По результатам анализа требований, предъявляемых к разрабатываемой СППР, глобальная цель системы (цель 0) была разделена на 3 базовых подцели. Далее представлена структура дерева целей. Все цели связаны отношением **И**. Цель под номером 2 не раскрывается, так как данная ветка будет подробно представлена позже.

0. Поддержка принятия решений по защите персональных данных – глобальная цель мультиагентной системы.
1. Ввод и хранение необходимых данных:
   1.1. Ввод и хранение свойств организации.
   1.2. Ввод и хранение свойств персональных данных.

1.3. Ввод и хранение свойств вычислительной сети.
1.4. Ввод и хранение свойств серверов.
1.5. Ввод и хранение свойств рабочих станций.
1.6. Ввод и хранение свойств программного обеспечения.
1.7. Ввод и хранение свойств информационных систем персональных данных.
1.8. Ввод и хранение свойств безопасности.
1.9. Ввод и хранение свойств документов на бумажных носителях.
2. Обеспечение безопасности персональных данных.
3. Управление безопасностью персональных данных:
3.1. Анализ изменений.
3.2. Анализ текущего уровня защищенности.
3.3. Мониторинг и ввод изменений:
3.3.1. Мониторинг и ввод изменений свойств организации.
3.3.2. Мониторинг и ввод изменений свойств персональных данных.
3.3.3. Мониторинг и ввод изменений процессов обработки персональных данных.
3.3.4. Мониторинг и ввод изменений свойств вычислительной сети.
3.3.5. Мониторинг и ввод изменений свойств аппаратного обеспечения.
3.3.6. Мониторинг и ввод изменений свойств программного обеспечения.
3.3.7. Мониторинг и ввод изменений свойств безопасности.
3.3.8. Мониторинг и ввод изменений нормативно-правовой базы.
3.4. Выполнение корректирующих действий:
3.4.1. Изменение структуры ИСПДн.
3.4.2. Изменение класса ИСПДн.
3.4.3. Изменение свойств ИСПДн.
3.4.4. Доработка, разработка моделей угроз.
3.4.5. Доработка, разработка моделей злоумышленника.
3.4.6. Изменение состава СЗПДн.

6. Уточнение целей. После того, как модель целей построена, ее необходимо детализировать для отображения динамики системы. Каждая цель детализируется при помощи техники, получившей название «анализ атрибутов-предшествования-переключения» (attribute-precede-trigger analysis) [6]. Уточненная модель для второй цели представлена на рис. 1.

Отношение предшествования (на модели *precedes*) показывает, что одна цель будет инициирована только после того, как другая цель будет выполнена. Отношение переключения (*triggers*) означает, что выполнение одной цели непосредственно инициирует выполнение другой цели, передавая при этом определенные параметры. Также для каждой цели указываются атрибуты, которые формируются в результате выполнения целей.

7. Моделирование организационных интерфейсов. На данном этапе описываются внешние объекты, с которыми взаимодействует система. К таким объектам могут относиться: пользователи, агенты иных систем, внешние ресурсы, внешние базы данных. Для каждого из объектов определяются протоколы, посредством которых он взаимодействует с системой.

Для СППР по защите персональных данных были определены следующие объекты:

- супервизор;
- администратор вычислительной сети;

- администратор информационных систем;
- администратор безопасности;
- руководитель структурного подразделения.

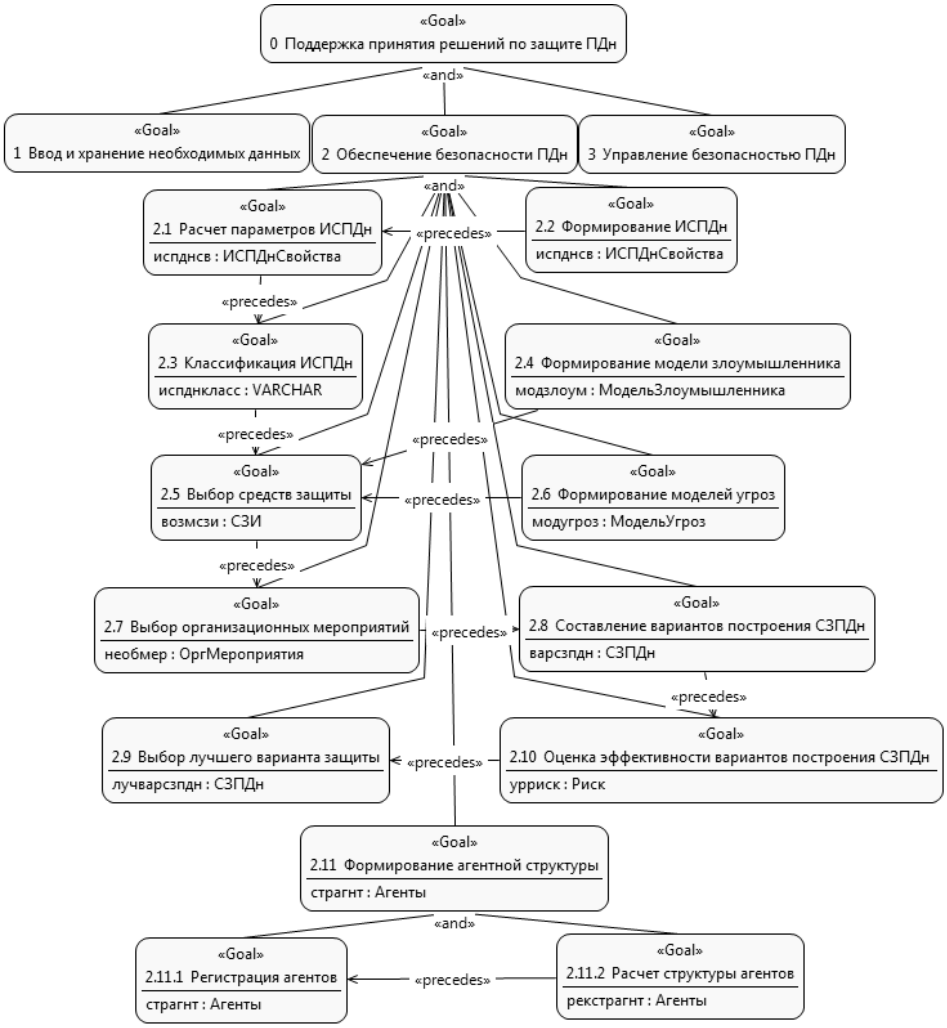

Рис. 1. Детализированная модель целей

Каждый из объектов взаимодействует системой посредством протоколов: ввода исходных данных, ввода изменений, вывода данных и подтверждения запросов.

8. Моделирование ролей. Моделирование ролей является одним из ключевых этапов построения МАС. На данном этапе определяются роли, выполняемые внутри системы, а также протоколы их взаимодействия между собой и с внешними объектами. Ролевая модель для СППР представлена на рис. 2.

Роли формируются таким образом, чтобы каждому листу дерева целей соответствовала своя роль. Для схожих целей допустимо наличие общей роли. Основная идея заключается в том, что для каждого внешнего объекта имеется соответствующая роль-интерфейс, которая отвечает за взаимодействие с пользователем и передачу управляющих команд другим ролям. Отдельная роль *АнализаторИзменений* отвечает за мониторинг изменений, их анализ и формирование соответст-

вующих запросов на выполнение корректирующих действий. Для каждой роли указываются цели, которые достигаются ролью. К сожалению, объем статьи не позволяет полностью описать ролевую модель.

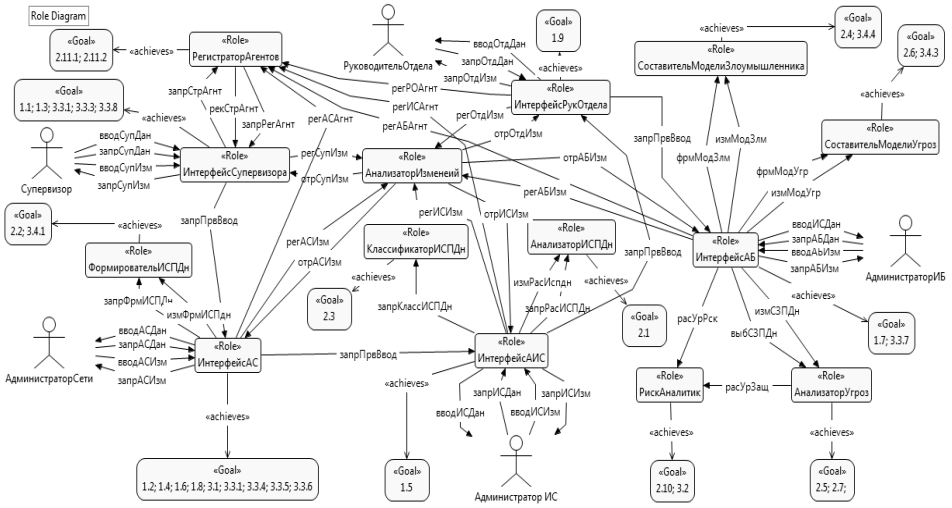

Рис. 2. Ролевая модель

9. Моделирование классов агентов. На этапе моделирования классов агентов формируется итоговая агентная структура системы. Класс агентов определяется путем группировки ролей, которые играет данный класс. Отношения между классами определяются отношениями между входящими в их состав ролями.

Для СППР по защите персональных данных были выделены следующие классы агентов:

- АгентСупервизора;
- АгентАдминистратораСети;
- АгентАдминистратораИС;
- АгентАдминистратораИБ;
- АгентРуководителяОтдела;
- АнализаторИзменений.

10. Моделирование протоколов. Целью данного этапа является определение деталей взаимодействия между ролями и агентами. Каждый протокол из *Модели классов агентов* описывается в терминах сообщений, передаваемых между агентами, либо между агентом и внешним объектом. Моделирование протоколов осуществляется в форме диаграмм взаимодействия AUML, которые позволяют указывать циклы сообщений, альтернативные взаимодействия и связь с другими протоколами. Сообщения имеют вид: *имя_сообщения(параметры)*.

11. Моделирование планов действий. На заключительном этапе проектирования представленного метода строятся модели планов действий, представляющие собой конечные автоматы. План действий отражает алгоритм, посредством которого агент достигает определенную цель. Минимальное количество планов агентов равно числу агентов, так как каждый агент должен выполнять, по меньшей мере, одно действие.

Согласно модели, в каждый момент времени агент может находиться в одном из состояний. Переход в состояние инициируется получением определенного сообщения. Во время нахождения в состоянии агент выполняет действия, связанные

с данным состоянием. В зависимости от результата выполнения действий агентом формируется то или иное сообщение. Деятельность агента заканчивается при достижении конечного состояния. На рис. 3 представлен пример *Модели плана действий*, осуществляющего регистрацию агента.

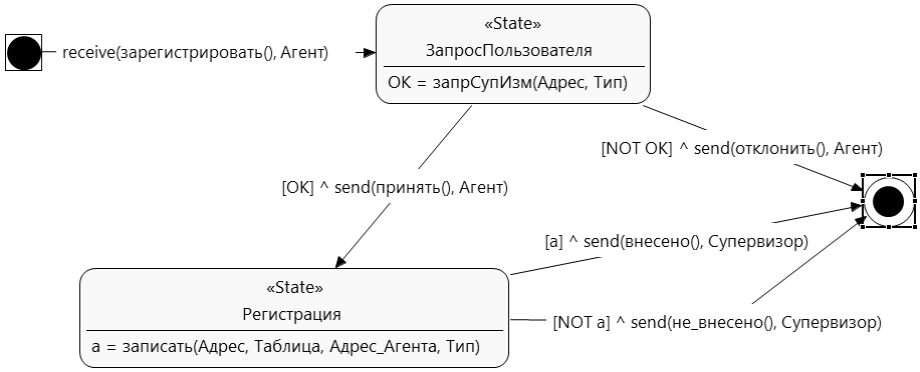

Рис. 3. Модель плана действий при регистрации агента

Заключение. В настоящее время является актуальной задача построения системы поддержки принятия решений по защите персональных данных, являющейся связующим звеном между высокоуровневыми нормативными документами и практической деятельностью по обеспечению безопасности персональных данных. Для этой цели хорошо подходит технология мультиагентных систем.

Проектирование подобной, достаточно сложной МАС требует применения специальной методологии. Ни одна из имеющихся на сегодняшний день методологий в полной мере не удовлетворяет предъявляемым требованиям, но наиболее подходящей является O-MASE. Разработанный на ее основе организационный подход предполагает замену ряда моделей набором онтологий. В соответствии с данным подходом построен комплекс моделей, описывающих проектируемую мультиагентную систему поддержки принятия решений по защите персональных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Белкин А.А., Чуприна С.И.* Проект MAD: Разработка мультиагентной системы обнаружения вторжений. Математика программных систем: Межвуз. сб. науч. ст. – Пермь: Перм. ун-т, 2006. – С. 123-134.
2. *Белков Н.В.* Построение системы защиты персональных данных. Проблемы и задачи. Актуальные проблемы в науке и технике. Т. 2. Информационные технологии. Сборник трудов пятой Всероссийской зимней школы-семинара аспирантов и молодых ученых, 17 – 20 февраля 2010 г. – Уфа: УГАТУ, 2011.– С. 57-60.
3. *Бондарь И.В., Гуменникова А.В., Золотарёв В.В., Попов А.М.* Система поддержки принятия решений по защите информации «Оазис» // Программные продукты и системы. – 2011. – № 3.
4. *Миков А.И., Замятина Е.Б., Панов М.П.* Мультиагентная система защиты распределенной имитационной модели с удаленным доступом. Advanced studies in software and knowledge engineering: Intern.Book Ser. № 4 (Suppl. Intern. J. Inform. Technol. Knowledge). Sofia: ITHEA, 2009. – Vol. 2. – P. 90-97.
5. *Chia-En Lin, Khrishna M. Kavi, Frederick T. Sheldon, Kris M. Daley and Robert K.* Abercrombie. A Methodology to Evaluate Agent-Oriented Software Engineering Techniques, Proceedings of IEEE HICS, Software Agents and Semantic Web Technologies Minitrack, IEEE Press, Hawaii, USA, 2007.

6. *DeLoach S.A. and García-Ojeda J.C.* O-MaSE: a customisable approach to designing and building complex, adaptive multi-agent systems, Int. J. Agent-Oriented Software Engineering, 2010. – Vol. 4, № 3. – P. 244-280.
7. *Garcia-Ojeda J.C., DeLoach S.A., Robby, Oyenan W.H. and Valenzuela J.* O-MaSE: a customizable approach to developing multiagent development processes, Agent-Oriented Software Engineering VIII: The 8th Intl. Workshop on Agent Oriented Software Engineering, LNCS. Springer, Berlin. –Vol. 4951. – P. 1-15.
8. *Scott A. DeLoach.* Developing a Multiagent Conference Management System Using the O-MaSE Process Framework, Proceedings of the 8th International Workshop on Agent Oriented Software Engineering, May 14, Honolulu, Hawaii, 2007.
9. *Scott A.* DeLoach. Engineering Organization-Based Multiagent Systems, Software Engineering for Multi-Agent Systems IV, Research Issues and Practical Applications, Lecture Notes in Computer Science 3914, Springer, 2006.

Статью рекомендовал к опубликованию к.т.н. А.А. Бакиров.

Васильев Владимир Иванович
Уфимский государственный авиационный технический университет.
E-mail: vasilyev@ugatu.ac.ru.
Республика Башкортостан, г. Уфа, ул. Карла Маркса, 12.
Тел.: 89173406400.
Зав. кафедрой вычислительной техники и защиты информации; д.т.н.; профессор.

Белков Николай Вячеславович
E-mail: unin68@gmail.com.
Аспирант кафедры вычислительной техники и защиты информации.

Vasilyev Vladmir Ivanovich
Ufa State Aviation Technical University.
E-mail: vasilyev@ugatu.ac.ru.
12, Karl Marks Street, Ufa, Bashkortostan Republic.
Phone: 89173406400.
Head of the Department Computer Engineering and Information Protection; Dr. of Eng. Sc.; Professor.

Belkov Nickolay Vacheslavovich
E-mail: unin68@gmail.com.
Postgraduate Student of Department Computer Engineering and Information Protection.