УДК 004.056

Н.В. Белков, В.И. Васильев

Поддержка принятия решений по обеспечению безопасности персональных данных на основе онтологического и мультиагентного подходов

Предложена поддержка принятия решений по обеспечению безопасности персональных данных на основе соответствующей экспертной системы. Сформулированы ключевые требования к системе. Разработана структура распределенной базы знаний системы поддержки принятия решений. Предложена методика проектирования мультиагентной системы поддержки принятия решений. Построен комплекс моделей проектируемой системы.

Ключевые слова: система поддержки принятия решений, персональные данные, онтология, мультиагентная система.

История вопроса защиты персональных данных

Идея о необходимости защиты персональных данных (ПДн) не нова. Еще в середине XX в. были приняты Всеобщая декларация прав человека и Международный пакт о гражданских и политических правах, гарантирующие неприкосновенность жилища, частной и семейной жизни, а также тайну корреспонденции.

Следующий этап начался в 70-е гогы и был связан с бурным развитием информационных технологий. Стало очевидно, что персональные данные, будучи однажды внесенными в информационные системы, впоследствии могут распространяться практически бесконтрольно. В ответ на новые угрозы в информационно развитых государствах появляются национальные и международные законодательства, регламентирующие порядок получения, обработки, хранения и передачи ПДн: резолюции Совета Европы, законы в Германии, Соединенных Штатах Америки, Франции и др. Начиная с 90-х годов национальные нормативные акты в области ПДн были приняты не только в странах Западной Европы, но и в государствах Восточной Европы, Азии и даже Африки. В настоящее время подобные законы действуют в 76 странах мира.

В Российской Федерации ФЗ № 152 «О персональных данных» принят в июле 2006 г. Помимо собственно Федерального закона, нормативную базу составляют методические документы ФСТЭК и ФСБ, а также ряд постановлений Правительства РФ. За прошедшие 6 лет в качестве операторов персональных данных зарегистрировалось порядка 240 тыс. организаций. В то же время в стране зарегистрировано около 4,5 млн юридических лиц, не считая индивидуальных предпринимателей. Таким образом, можно предположить, что не более 5% организаций выполняют необходимые мероприятия по защите обрабатываемых ПДн.

Постановка задачи

Ситуация, сложившаяся в Российской Федерации в части защиты ПДн, во многом связана с особенностями ПДн как информации ограниченного доступа. На рис. 1 представлена модель проблемной области.

Как правило, на предприятии одновременно обрабатываются несколько групп ПДн различных категорий и различного объема. При этом обработка ведется сразу в нескольких информационных системах персональных данных (ИСПДн), которые могут охватывать как одну рабочую станцию, так и несколько подразделений или даже территориальных отделений. Каждая ИСПДн имеет собственный набор уязвимостей и параметров, а значит, и перечень возможных угроз. В условиях подобного разнообразия необходимо для каждой ИСПДн осуществить выбор мер по защите ПДн, перекрывающих все актуальные угрозы и ведущих к минимизации рисков. Руководству приходится решать проблему защиты ПДн в достаточно жестких рамках ограничений финансовых и трудовых ресурсов, поскольку в данный процесс необходимо вовлекать большое число квалифицированных специалистов, а услуги сторонних организаций требуют значительных материальных затрат. Для организации безопасности ПДн собственными силами предприятиям требуется соответствующая экспертная система. Таковой системой является проектируемая система поддержки принятия решений (СППР) по обеспечению и управлению безопасностью персональных данных.

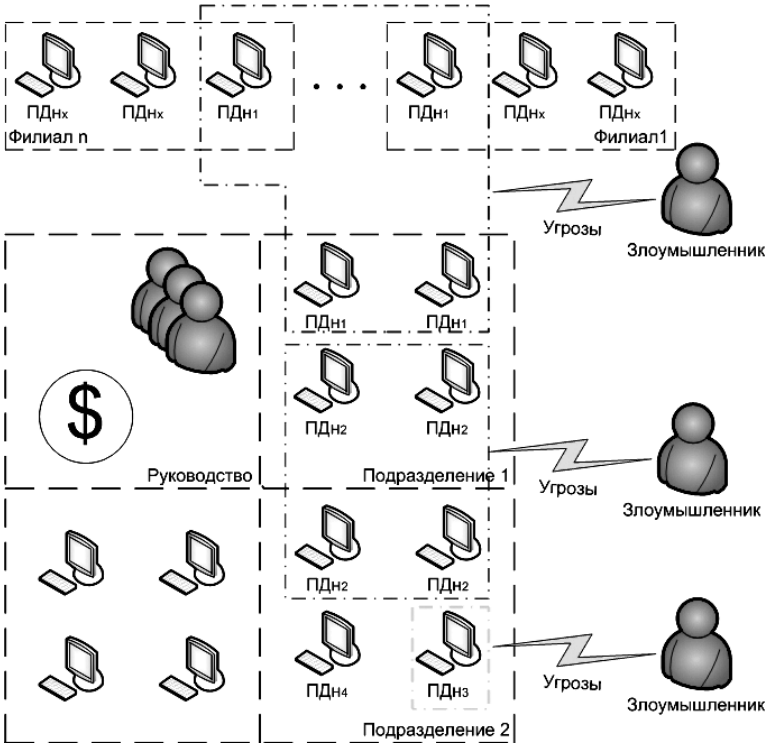

Рис. 1. Модель проблемной области защиты ПДн

Для построения СППР необходимо решить ряд ключевых задач:

1) Разработать комплекс моделей, описывающих целевую систему.

2) Разработать алгоритмическое обеспечение процесса принятия решений и структуру базы знаний СППР.

Требования к СППР по обеспечению и управлению безопасностью ПДн можно сформулировать на основе международного стандарта ИСО/МЭК 27001. При этом весь процесс можно представить в виде цикла Демминга, на каждом из этапов которого определяются необходимые функциональные возможности системы [1, 2].

Этап планирования (Plan):

- систематизация необходимых сведений об информационной системе и процессах обработки ПДн;
- формирование ИСПДн из имеющихся автоматизированных систем;
- классификация ИСПДн.

Этап осуществления (Do):

- построение моделей угроз и моделей злоумышленника для ИСПДн;
- формирование вариантов построения системы защиты ПДн (СЗПДн);
- анализ рисков безопасности ПДн;
- выбор наилучшего варианта СЗПДн.

Этап проверки (Check):

- оценка текущего уровня риска и эффективности реализованных мероприятий;
- мониторинг изменений ИСПДн и процессов обработки ПДн;
- анализ изменений и выбор реакции на них.

Этап действия (Action):

- выполнение корректирующих действий.

Онтологический подход к построению СППР

При проектировании СППР был проведен анализ основных направлений исследований в области построения интеллектуальных систем. С учетом особенностей проблемной области за основу выбрано два основных подхода: онтологический и мультиагентный.

Онтологический подход подразумевает построение комплекса онтологий в качестве моделей представления знаний СППР. Термин «онтология» пришел в инженерию из философии и впервые

появился в работе Томаса Грубера [3]. Грубер дает следующее определение: «Онтология – формальная спецификация разделяемой концептуализации». Другими словами, она формально описывает некоторую предметную область в терминах классов объектов, их атрибутов и связей между ними. Математически онтология может быть представлена в виде кортежа:

$$\mathbf{O} = < \mathbf{C}, \mathbf{Pr}, \mathbf{V}, \mathbf{I}, \mathbf{R}, \mathbf{F} >, \quad (1)$$

где **C** – множество классов концептов предметной области; **Pr** – множество свойств классов; **V** – множество значений свойств; **I** – множество экземпляров классов; **R** – множество отношений между классами; **F** – множество аксиом, заданных на классах концептов.

Для СППР по обеспечению безопасности персональных данных были разработаны онтологии трех уровней, образующих иерархическую структуру, представленную на рис. 2.

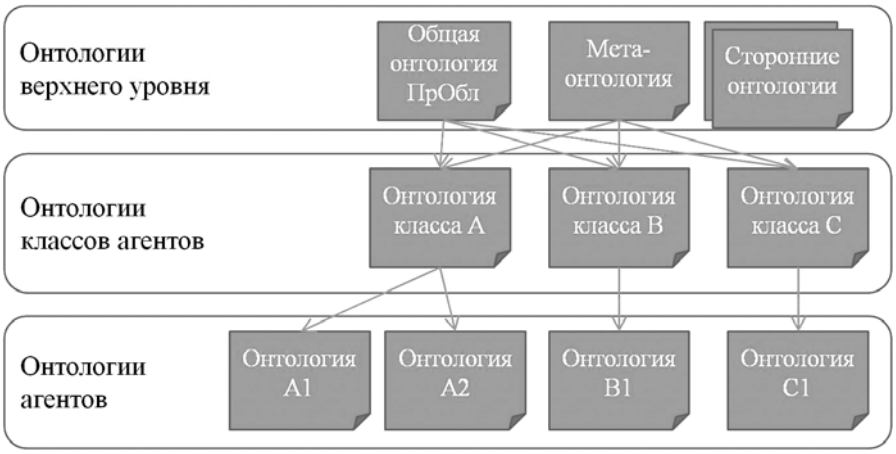

Рис. 2. Иерархия онтологий СППР

На верхнем уровне располагаются две онтологии:

- общая онтология предметной области;
- метаонтология.

Общая онтология предметной области содержит все знания в области обработки и защиты персональных данных, необходимые для принятия решений. Это такие классы концептов, как персональные данные, субъект персональных данных, угроза, рабочая станция, документ и др. При этом в общую онтологию не вносятся знания о конкретных объектах защиты. На рис. 3 изображен фрагмент общей онтологии, представленной в виде многосвязного графа. Метаонтология содержит знания, описывающие работу системы в целом и содержащие такие концепты, как роль, протокол, агент, алгоритм и т.д. Кроме того, предполагается возможность импорта на верхнем уровне сторонних онтологий в целях организации межсистемного взаимодействия.

На основе онтологий верхнего уровня формируются онтологии классов агентов СППР. Они представляют собой объединение фрагментов высокоуровневых онтологий, содержащих только знания, необходимые конкретным классам агентов мультиагентной системы. Наконец, на нижнем уровне находятся онтологии отдельных агентов, являющиеся экземплярами онтологий классов агентов, дополненные знаниями о конкретных объектах защиты. Онтологии агентов становятся не только хранилищами знаний, но и хранилищами данных.

Использование онтологий в целом и трехуровневой их модели в частности позволяет:

- организовать единообразное представление знаний, общее для всех агентов;
- представить плохо формализуемые знания в виде формальной структуры, пригодной для машинной обработки;
- уменьшить объем баз знаний отдельных агентов, сократив время, необходимое для принятия решения;
- снизить зависимость знаний от программного кода, что повышает гибкость СППР;
- организовать взаимодействия со сторонними информационными системами.

Мультиагентный подход к построению СППР

При мультиагентном подходе СППР формируется не как единая интеллектуальная система, а как множество взаимодействующих интеллектуальных агентов. Классические методики проектиро-

вания информационных систем и программного обеспечения плохо применимы при создании мультиагентных систем (МАС). По этой причине в последние годы активно разрабатываются специализированные методологии проектирования МАС.

Рис. 3. Фрагмент общей онтологии предметной области

В рамках исследования был проведен анализ наиболее популярных из них: Gaia, Tropos, Prometheus, MASE и O-MASE. Каждая из представленных методологий имеет некоторые недостатки [1]. Так, методологии Gaia и MASE не предлагают средств моделирования предметной области, в Prometheus и Tropos не поддерживается проверка согласованности моделей и протоколов, причем Tropos вообще не подразумевает моделирование протоколов и динамики системы. Также в Gaia отсутствуют этапы низкоуровневого проектирования, а в Prometheus – стадии описания требований и целей системы. Ни одна из представленных методологий не предусматривает использования онтологий. По результатам анализа было принято решение о доработке одной из исследуемых методологий. Для этих целей выбрана O-MASE как наиболее полная и законченная.

Фактически O-MASE предоставляет разработчику набор этапов проектирования и рекомендации по их объединению в единый метод [4]. Перечень предлагаемых методологией этапов представлен в таблице. Исходная методология доработана путем исключения из нее ряда этапов и добавления этапов построения онтологий.

При формировании общих требований к СППР было принято решение, что агенты будут представлять определенные должностные лица, вовлеченные в процесс обработки и защиты ПДн. 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. 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». Также 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. Все необходимые требования и ограничения будут определены в онтологиях. Онтологии также содержат подробное описание предметной области, что позволяет исключить не только фазу моделирования политик, но и фазу

моделирования предметной области. Вместо них добавляются этапы построения онтологий различного уровня и разработки баз знаний агентов.

Этапы исходной и предлагаемой методологий

Исходная методология	Предлагаемая методология
1. Описание требований	1. Описание требований
2. Моделирование целей	2. Построение онтологий верхнего уровня
3. Уточнение целей	3. Моделирование целей
4. Моделирование предметной области	4. Уточнение целей
5. Моделирование организационных интерфейсов	5. Моделирование организационных интерфейсов
6. Моделирование ролей	6. Моделирование ролей
7. Детализация ролей	7. Моделирование классов агентов
8. Моделирование классов агентов	8. Построение онтологий классов агентов
9. Моделирование протоколов	9. Моделирование протоколов
10. Моделирование политик	10. Моделирование планов действий
11. Моделирование планов действий	11. Разработка баз знаний агентов
12. Моделирование возможностей	12. Генерация программного кода
13. Моделирование операций	–
14. Генерация программного кода	–

Часть этапов, таких как описание требований и построение онтологий, рассматривалась выше. На остальных этапах осуществляется формирование тех или иных моделей. Так, целью моделирования ролей является преобразование исходных требований к системе в совокупность структурированных целей, достигаемых системой. Модель целей представляет собой дерево целей, связанных между собой отношениями «И/ИЛИ». 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. Для рассматриваемой СППР исходная цель разбита на 3 подцели, связанные отношением «И»:

- Цель 1. Систематизация необходимых данных (9 подцелей).
- Цель 2. Обеспечение безопасности ПДн (13 подцелей).
- Цель 3. Управление безопасностью ПДн (16 подцелей).

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). Отношение предшествования (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.

На этапе моделирования организационных интерфейсов определяются внешние объекты, взаимодействующие с системой, и протоколы взаимодействия с ними. В качестве таковых объектов для СППР выделяются пользователи, каждый из которых взаимодействует с системой посредством протоколов ввода данных и команд, вывода данных и формирования запросов:

- супервизор;
- администратор вычислительной сети;
- администратор информационных систем;
- администратор безопасности;
- руководитель структурного подразделения.

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. Роли формируются таким образом, чтобы каждому листу дерева целей соответствовала своя роль. Для схожих целей допустимо наличие общей роли. В результате моделирования выделены роли:

- интерфейсы пользователей;

- формирователь ИСПДн;
- классификатор ИСПДн;
- анализатор ИСПДн;
- составитель моделей угроз и злоумышленника;
- анализатор угроз;
- риск-аналитик;
- анализатор изменений;
- регистратор агентов.

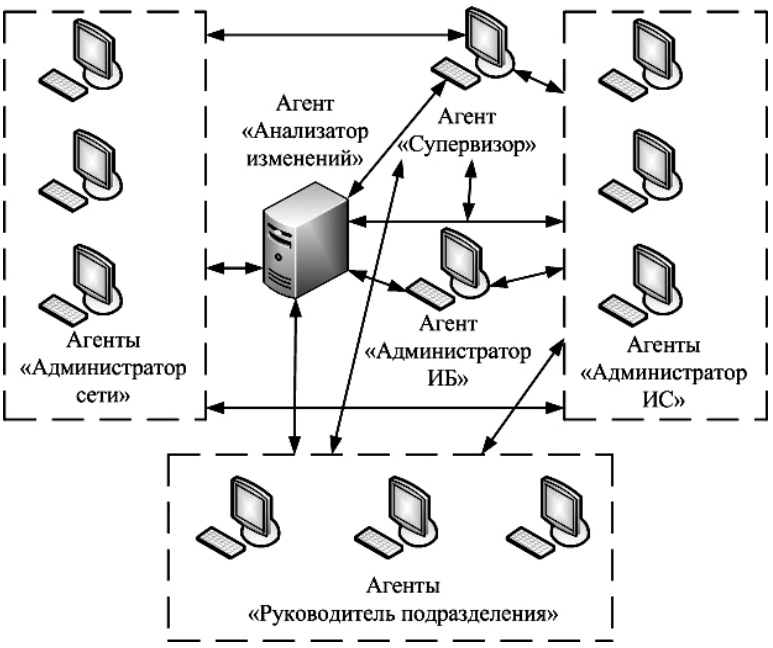

Рис. 4. Общая структура СППР

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. Общая структура мультиагентной СППР по обеспечению безопасности ПДн отображена на рис. 4.

Целью этапа моделирования протоколов 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)».

Наконец, на этапе моделирования планов действий 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, т.к. 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.

Все агенты за исключением агента «Анализатор изменений» имеют схожую архитектуру (рис. 5).

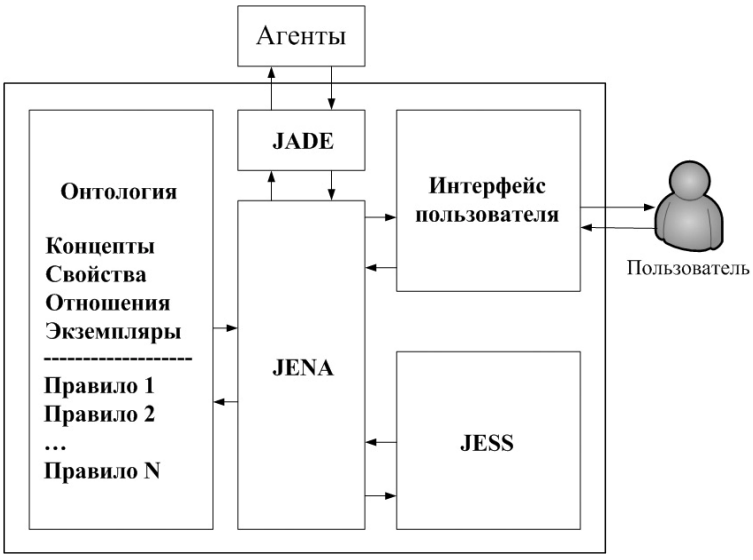

Рис. 5. Архитектура агентов, взаимодействующих с пользователями

Центральное место занимает онтология, в которой содержатся концепты, свойства, отношения, экземпляры, а также SWRL-правила (Semantic Web Rule Language), представляющие собой дизъюнкты Хорна. Для получения новых знаний используется машина вывода JESS, в которую вводятся данные и правила из онтологии. Работа с онтологиями осуществляется средствами библиотеки JENA, а межагентное взаимодействие – средствами библиотеки JADE.

Заключение

1. Сформулированы ключевые требования к СППР по обеспечению безопасности ПДн на различных этапах жизненного цикла.

2. Разработана распределенная база знаний СППР по обеспечению безопасности ПДн, образованная трехуровневой системой онтологий.

3. Предложена методика проектирования мультиагентных систем, основанная на методологии O-MASE и включающая этапы онтологического моделирования. Построен комплекс моделей, необходимых для построения СППР.

4. Разработан исследовательский прототип СППР по обеспечению безопасности персональных данных, которая позволяет операторам ПДн, не имеющим в своем штате специалистов в области информационной безопасности, самостоятельно разрабатывать системы защиты персональных данных. Применение данной СППР позволяет снизить суммарные финансовые и временные затраты на обеспечение безопасности ПДн.

Литература

1. Белков Н.В. Организационный подход к проектированию мультиагентной системы поддержки принятия решений по защите персональных данных / Н.В. Белков, В.И. Васильев // Известия ЮФУ. Технические науки (Таганрог). – 2011. – №12 (125). – С.14–24.

2. Белков Н.В. Автоматизированное моделирование угроз и анализ рисков безопасности персональных данных // Информационные технологии и системы: матер. Первой междунар. конф., Банное (28 февраля – 4 марта 2012 г.). – Челябинск: Изд-во Челяб. гос. ун-та, 2012. – С. 63–64.

3. Лапшин В.А. Онтологии в компьютерных системах. – М.: Научный мир, 2010. – 224 с.

4. DeLoach S.A. O-MaSE: a customisable approach to designing and building complex, adaptive multi-agent systems / S.A. DeLoach, J.C. García-Ojeda // Int. J. Agent-Oriented Software Engineering. – Vol. 4, № 3. – P. 244–280.

Белков Николай Вячеславович
Аспирант каф. вычислительной техники и защиты информации Уфимского государственного авиационного технического университета (УГАТУ)
Тел.: 8 (917) 340-64-00
Эл. почта: unin68@gmail.com

Васильев Владимир Иванович
Д-р техн. наук, проф., зав. каф**.** вычислительной техники и защиты информации УГАТУ
Тел.: 8 (347) 273-06-72
Эл. почта: vasilyev@ugatu.ac.ru

Belkov N.V., Vasilyev V.I.

Decision support for personal data security based on ontological and mutli-agent approaches

Decision support for personal data security by the corresponding expert system is offered. Key system requirements are specified. The structure of a distributed knowledge base of the decision support system is developed. A method for multi-agent decision support system designing is suggested. The complex of models for the designed system is formed.

Keywords: decision support system, personal data, ontology, multi-agent system.