18. *Lebedeva A.V., Ryabov V.M.* O chislennom reshenii sistem lineynykh algebraicheskikh uravneniy s plokho obuslovlennymi matritsami [On the numerical solution of systems of linear algebraic equations with ill-conditioned matrices], *Vestnik Sankt-Peterburgskogo universiteta. Matematika. Mekhanika. Astronomiya* [Bulletin of St. Petersburg University. Maths. Mechanics. Astronomy], 2019, No. 4, pp. 619-625.
19. *Böttcher A.; Grudsky S.* Toeplitz Matrices, Asymptotic Linear Algebra and Functional Analysis. Basel: Birkhäuser, 2012, 112 p.
20. *Friedrich L. Bauer.* Origins and Foundations of Computing: In Cooperation with Heinz Nixdorf MuseumsForum. Berlin: Springer Berlin Heidelberg, 2010, 142 p.
21. *Shterenliht D.V.* Gidravlika [Hydraulics]. Moscow: Izd-vo Kolos-S, 2009, 656 p.

Статью рекомендовал к опубликованию д.т.н., профессор М.Ю. Медведев.

Долгой Вячеслав Евгеньевич – Южный федеральный университет; e-mail: vedolgoy@sfedu.ru; г. Таганрог, Россия; тел.: 89081841211; кафедра высшей математики; старший преподаватель.

Гамолина Ирина Эдуардовна – e-mail: iegamolina@sfedu.ru; тел. 89185190837; кафедра высшей математики; к.т.н.; доцент.

Dolgoy Vyacheslav Evgenievich – Southern Federal University, e-mail: vedolgoy@sfedu.ru; Taganrog, Russia; phone: +79081841211; the department of higher mathematics; senior lecturer.

Gamolina Irina Eduardovna – e-mail: iegamolina@sfedu.ru; phone: +79185190837; the department of higher mathematics; cand. of eng. sc.; associate professor.

УДК 004.822 DOI 10.18522/2311-3103-2022-5-37-47

П.Ю. Чудинов, Л.К. Бабенко, Ю.И. Рогозов

АНАЛИЗ ПРОБЛЕМ ЗАЩИТЫ ИНФОРМАЦИИ В СЕМАНТИЧЕСКИХ СЕТЯХ

Анализируется структура, принципы и технологи, используемые при создании семантических сетей, методика представления знаний в семантической сети. Отдельное внимание уделяется анализу структуры запросов к данным, хранящихся в семантической сети. Целью анализа является определение структурных элементов, несущих в себе конфиденциальную, либо иную важную информацию для дальнейшего формирования методологии её защиты с учётом специфики семантической сети. В результате анализа типовых структур семантических сетей рассмотрены основополагающие структурные элементы и понятия, составляющие структуру анализируемого метода представления знаний. Определены используемые для её построения специализированные языки и структура информационного запроса к базе знаний, в которой были выявлены элементы, несущие конфиденциальную информацию и потенциально уязвимые к атакам злоумышленников. Выявлены проблемы в информационной безопасности семантических сетей, такие как: незащищённость от вредоносных запросов SPARQL, которая может быть использована для получения информации из семантической сети без соответствующих привилегий и доступов; уязвимость данных в передаваемом информационном запросе, характеризующаяся слабой ориентированностью существующих методов защиты на специфику семантических сетей; проблема оценки уровня доверия к получаемым данным семантической сети. Одним из подходов для решения этих проблем может являться создание распределённой системы оценивания доверия к узлам и данным в семантической сети, а также реализация механизмов защиты информации и информационных запросов. Полученные в результате анализа результаты о структуре передаваемых данных являются неотъемлемой частью процесса разработки средств защиты информации в семантических сетях.

Семантическая сеть; онтология; граф; RDF; OWL; SPARQL; представление знаний; информационный запрос.

P.Y. Chudinov, L.K. Babenko, Y.I. Rogozov

ANALYSIS OF PROBLEMS OF INFORMATION PROTECTION IN SEMANTIC NETWORKS

The article analyzes the structure, principles and technologies used in the creation of semantic networks, the methodology for representing knowledge in a semantic network. Special attention is paid to the analysis of the structure of queries to data stored in the semantic network. The purpose of the analysis is to determine the structural elements that carry confidential or other important information for the further formation of a methodology for its protection, considering the specifics of the semantic network. As a result of the analysis of typical structures of semantic networks, the fundamental structural elements and concepts that make up the structure of the analyzed method of knowledge representation are considered. The specialized languages used for its construction and the structure of the information request to the knowledge base are determined, in which elements carrying confidential information and potentially vulnerable to attacks by intruders were identified. Problems in the information security of semantic networks have been identified, such as: exposure to malicious SPARQL queries, which can be used to obtain information from the semantic network without appropriate privileges and accesses; data vulnerability in the transmitted information request, characterized by a weak focus of existing protection methods on the specifics of semantic networks; the problem of assessing the level of confidence in the received data of the semantic network. One of the approaches to solve these problems can be the creation of a distributed system for evaluating the trust in nodes and data in the semantic network, as well as the implementation of mechanisms for protecting information and information requests. The results obtained as a result of the analysis on the structure of the transmitted data are an integral part of the process of developing information security tools in semantic networks.

Semantic web; ontology; graph; RDF; OWL; SPARQL; knowledge representation; information query.

Введение. В настоящее время семантические сети являются перспективным средством для создания сложных информационных систем, способных, например, формировать некие выводы на основе данных. Но в отличие от альтернативных технологий, например, на основе блокчейна, семантическая сеть не имеет хорошо развитой политики конфиденциальности и безопасности [1]. Это достаточно критично для веб-стандарта, который используется для создания информационных систем, объединяющих большое количество данных из разных источников. Для того, чтобы исправить недостатки в информационной безопасности семантической сети, требуется провести серьезный анализ и внимательно отнестись к работам исследователей в данной области.

Семантическая сеть – это, по сути, граф, узлы которого помечены атомарными формулами, а дуги представляют собой отношения между ними. Узлы этого графа затем представляют сущности и классы сущностей. Эти классы затем могут быть иерархически упорядочены для представления знаний [2]. Это приводит к двум основным отношениям между узлами, а именно: подкласс, сущность. Методы семантических сетей были впервые разработаны как метод представления человеческих знаний. Основой построения семантической сети являются онтологии, языки запросов, основанные на онтологиях Структура включает механизмы вывода, предназначенные для таких операций, как наследование. Эти механизмы состоят из двух частей. Одна из них имеет дело с правилами с помощью прямой цепочки, обратной цепочки или каким-либо другим методом. Другая часть будет обрабатывать сетевые операции, сопоставляя соответствующие ссылки в сети, чтобы вывести найденные факты.

В статье анализируется структура, специальные языки запросов, правила формирования логических выводов. Проведение такого анализа, определение средств и методик построения семантических сетей, анализ структуры информационных запросов и потенциальных уязвимостей – являются обязательными шагами на пути к разработке средств защиты информации в семантических сетях.

Постановка задачи. Целью работы является разработка облика средств защиты информации на основании анализа принципов функционирования семантических сетей, определения логических элементов и технологий, участвующих в информационных процессах семантической сети, а также определение данных, которые могут нести важную, либо конфиденциальную информацию и при этом потенциально уязвимых к несанкционированному доступу.

1. Анализ основ построения семантической сети. Проблема проверки на вредоносность информационных запросов. Семантической сетью является структура данных, имеющая определенный смысл и организованная в определённом порядке. Стандартного определения семантической сети не существует, но обычно под ней подразумевают, что семантическая сеть – это система знаний, имеющая определенный смысл в виде целостного образа сети, узлы которой соответствуют понятиям и объектам, а дуги – отношениям между понятиями и объектами [3].

Всевозможные подсети, входящие в состав семантической сети, можно рассматривать как самостоятельные сети. В том числе к ним могут быть отнесены и сетевые структуры моделей баз данных. Например, на рис. 1 представлена довольно простая семантическая сеть, однако, она интересна тем, что на ней представлен пример объединения двух понятий (Airbus A320 и орёл) из двух совершенно разных предметных областей, но имеющих общие свойства и качества.

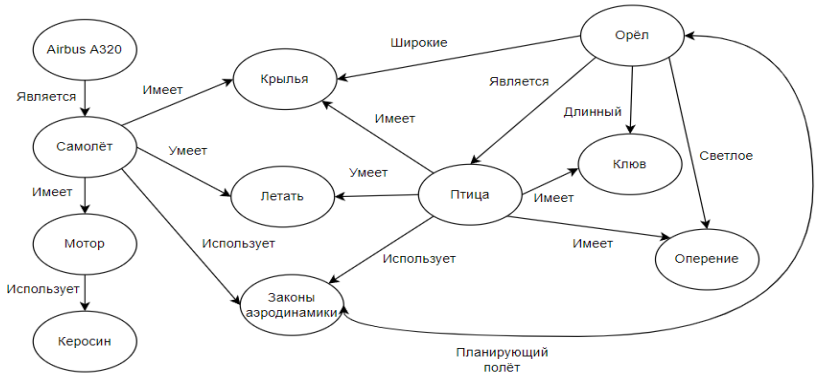

Рис. 1. Пример семантической сети

Сама по себе семантическая сеть является моделью памяти и не раскрывает, каким образом осуществляется представления знаний. Поэтому семантические сети должны рассматриваться как метод представления знаний с возможностями структурирования этих знаний, процедурами их использования и механизмом вывода [4].

Семантическая сеть представляет собой ориентированный граф с помеченными дугами и вершинами. Основными элементами сети являются вершины и дуги. При этом вершинам семантической сети соответствуют понятия, события и свойства [5]:

♦ Понятия – представляют собой сведения об абстрактных или физических объектах предметной области или реального мира.

♦ События – представляют собой действия, происходящие в реальном мире, и определяются:

- указанием типа действия;
- указанием ролей, которые играют объекты в этом действии.

♦ Свойства – используются для уточнения понятий и событий. Применительно к понятиям они описывают их особенности и характеристики (цвет, размер, качество и т.д.), а применительно к событиям – продолжительность, время, место.

Точно так же, как реляционным базам данных нужен специальный язык запросов SQL, семантическая сеть данных, обычно представляемая с использованием RDF (Resource Description Framework) в качестве формата данных, нуждается в собственном, специфичном для RDF языке запросов. Для обеспечения этой потребности используется язык запросов SPARQL (Simple Protocol and RDF Query Language).

Технически запросы SPARQL основаны на так называемых тройных шаблонах. RDF можно рассматривать как набор отношений между ресурсами (тройная модель RDF). Запросы в SPARQL предоставляют один или несколько шаблонов для таких отношений. Эти тройные шаблоны аналогичны тройкам RDF, за исключением того, что одна или несколько составляющих ссылок на ресурсы являются переменными [6].

Используя SPARQL, пользователи сети данных могут извлекать различную информацию, которая возвращается, например, в формате таблицы, которая затем, при необходимости, может быть подвергнута дальнейшей обработке и анализу [7]. При таком подходе SPARQL предоставляет собой мощный инструмент для создания, например, сложных сайтов или поисковых систем, а также информационных систем, способных с применением определённых правил проводить анализ имеющихся данных, и делать на основании этого некоторые логические выводы.

На рис. 2 представлена схема клиент-серверного взаимодействия в типичной семантической сети, основанной на правилах. С помощью пользовательского интерфейса клиент получает доступ к взаимодействию, например, со значениями определённых переменных. Задав значения этих переменных, их можно обработать соответствующим логическим модулем информационной системы, а затем, используя логические правила на языке SPARQL, выбрать нужные источники данных из базы данных RDF [8].

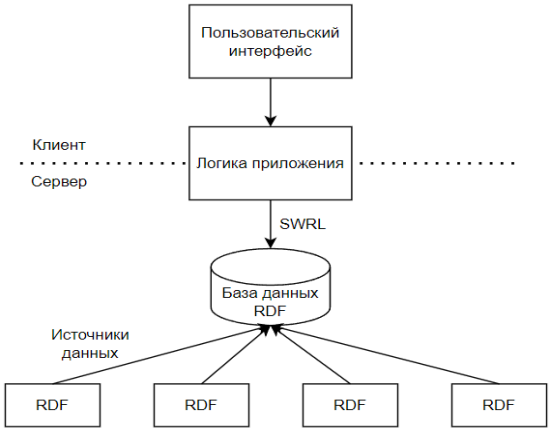

Рис. 2. Структура клиент-серверной архитектуры ИС с доступом к семантической сети

SPARQL можно использовать как часть общей среды программирования, но запросы также можно отправлять в виде сообщений на удалённые конечные точки с использованием сопутствующих технологий. Используя такие конечные точки SPARQL, приложения могут запрашивать удалённые данные RDF и даже создавать новые RDF-графы без какой-либо дополнительной нагрузки на сервер [6].

С точки зрения безопасности для запросов остаются нерешёнными такие проблемы, как атаки, основанные на инъекциях вредоносного кода в запрос SPARQL. Подобная угроза существует и в языке запросов SQL, однако, в SPARQL в отличии от SQL проводилось гораздо меньшее количество исследований. Так в работе [9] отмечается малое количество работ, посвящённых этой проблеме, которые лишь ограниченно или поверхностно затрагивают эту тему. В работе [10] также отмечается незначительное количество работ, направленных на последствия для безопасности после применения технологии семантических сетей в различных системах. В таких работах конфиденциальность данных рассматривалась как отдельная, специфическая и часто чисто техническая задача, связанная чаще всего только с идентификацией, либо сбором или доступом к данным. За некоторыми исключениями, очень немногие работы действительно рассматривают потенциал технологий семантической сети. В работе [11] отмечается низкая эффективность существующих предложений по защите семантических сетей. По-прежнему требуется повышение производительности алгоритмов оценки уровня доверия и более полная интеграция и взаимодействие различных подходов к управлению доступом. Таким образом, на настоящий момент отсутствуют эффективные средства защиты и контроля запросов в семантических сетях.

2. Анализ структуры запросов в семантической сети. Проблема безопасности данных в информационных запросах. Семантическая сеть основана на связанных данных, в которых необходимые элементы идентифицируются с помощью URI (унифицированный идентификатор ресурса). Из-за такого подхода семантическая сеть в значительной степени зависит от способности этих идентификаторов успешно извлекать документы, иначе семантическую сеть нельзя было бы назвать сетью [1].

База данных хранит семантические данные и онтологии, позволяет запрашивать семантические данные и выполнять запросы с помощью онтологий к реляционным данным, а также использовать предоставляемые или определяемые пользователем логические выводы для расширения возможностей запросов к семантическим данным.

На рис. 3 отражено, как взаимодействуют функции хранения, запросов и логических выводов. Структура содержит в себе четыре компонента, помеченные как логический модуль, запрос данных, хранилище и база данных [12].

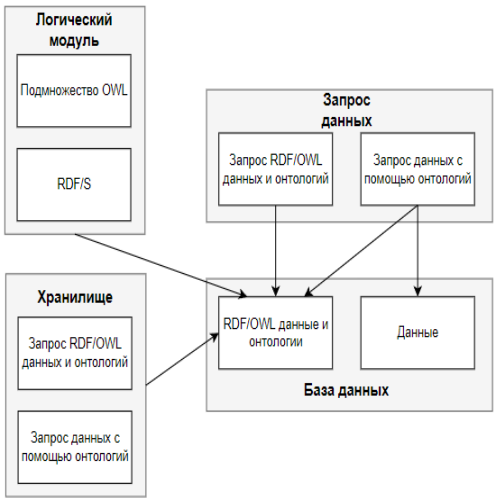

Рис. 3. Структура взаимодействия элементов семантической сети с базой данных

Как показано на рис. 1, база данных содержит семантические данные и онтологии. Наиболее эффективным подходом для загрузки семантических данных является массовая загрузка, но также можно загружать данные постепенно, используя транзакционные операторы логического модуля. Таким образом, можно запрашивать семантические данные, а также выполнять запросы семантических и традиционных реляционных данных с помощью онтологий для поиска семантических отношений.

При анализе кода обработки поиска для функции запроса, представленного на рис. 4, авторами статьи [9], что структура запроса SPARQL разделена на зарезервированные слова SPARQL, переменные SPARQL, отношения онтологий, которые представлены URI, знаки препинания SPARQL и переменная PHP.

Согласно анализу [9], слабым местом запроса SPARQL, с точки зрения информационной безопасности является переменная PHP, которая должна получать значение заполненного поля ввода от пользователя без проверки того, каким может был произведён этот код и не находятся ли в нём элементы потенциально вредоносного кода.

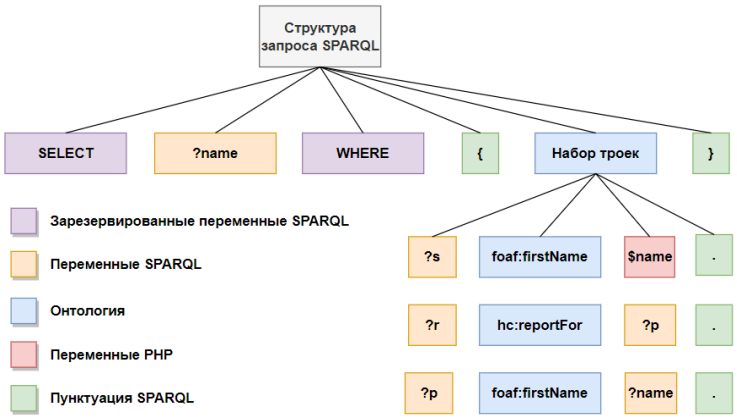

Рис. 4. Анализ структуры запроса SPARQL

Рассмотрим некоторые проблемы, связанные со структурой запросов. В работе [13] отмечается ограниченность реализации безопасности тройки RDF в том, что нет возможности реализовать ограничение доступа, например, к конкретному объекту для конкретного пользователя. Также, часто используемые для контроля доступа метаданные RDF не обеспечивают защиты, так как возвращают результат в виде обычного текста, который, таким образом, может быть перехвачен. В работе [9] проводилось исследование инъекций в запрос SPARQL и было установлено, что в переменную PHP, отвечающую за хранение имени в наборе троек, может быть встроен потенциально вредоносный код, с помощью которого можно получить доступ к конфиденциальной информации. Авторы работы [14] уделяют внимание таким проблемам, как ориентированные только на синтаксис средства безопасности XML; отсутствие средств защиты для онтологий, не зависящих от синтаксиса; отсутствие ассоциативной защиты конфиденциальных данных, которые могут быть связаны с другими открытыми данными и могут появляться вместе.

3. Стек семантической сети. Проблема определения уровня доверия. Стек семантической сети используется для визуального отображения архитектуры семантической сети, состоящей из многоуровневых протоколов. Функции и отношения между различными компонентами показаны на рис. 5 [15]:

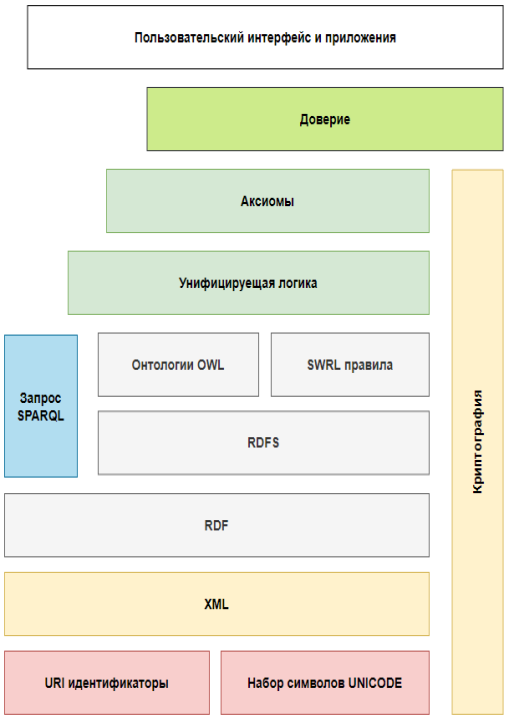

Рис. 5. Структура ИС, основанной на семантической сети

XML – это синтаксический уровень семантической сети. XML – это язык разметки, который организует данные в виде тегов. Вложенная структура тегов определяет взаимосвязь данных в документе. XML не имеет фиксированного набора тегов, теги определяются пользователями, поэтому XML очень гибкий и может использоваться в качестве метаязыка языка разметки [16].

RDF – это уровень обмена данными в семантической сети. RDF – это модель данных, используемая для описания ресурсов в интернете и взаимосвязи между ресурсами [17]. Её цель – установить общую структуру для описания сетевых ресурсов. RDF решает проблему, заключающуюся в том, что грамматика XML не может описывать семантику.

OWL – это язык онтологии семантической сети. Этот язык используется для построения онтологии, связанной с исследуемой областью. На основе схемы RDF в OWL создаётся словарь для описания классов и свойств, таких как дизъюнктивность классов, ограничения мощности, логические комбинации классов, более обширные свойства и свойства свойств, а также классы перечисления [18].

Хотя онтология, организованная в виде семантической сети, очень хорошо отражает структуру исследуемой предметной области, языка OWL далеко не достаточно для работы со свойствами объектов и формирования каких-либо рассуждений. Для полноценной работы онтологии её нужно научить делать эти самые логические суждения. На помощь здесь приходят правила.

Правило – это формула (1) образа:

$$\varphi 1 \Lambda \ldots \Lambda \varphi k \rightarrow \Psi, \quad (1)$$

где $\varphi 1 \Lambda \ldots \Lambda \varphi k \rightarrow \psi$ – проверяемые условия, а ψ – некий вывод. Смысл правила заключается в том, что всякий раз, когда условия истинны, то вывод, вытекающий из совокупности этих условий, тоже принимает значение истинно.

SWRL (язык правил семантической паутины) – это формат обмена правилами семантической сети. SWRL разработан для того, чтобы восполнить неспособность логических суждений языка OWL. SWRL правила описывают знания онтологии OWL с помощью высоко абстрактного синтаксического выражения, которое реализует собой комбинацию между правилами знаниями OWL и некими логическими выводами, следующими из совокупности значений определённых свойств.

Не стоит забывать, что онтологии, применяемые в реальных условиях, постоянно развиваются [19], соответственно, требования к ним постоянно меняются. Некоторые онтологические знания перестают иметь отношения к предметной области или становятся незначительными и ненужными для проведения рассуждений. В этом случае это знание необходимо удалить из онтологии. Подобным образом необходимо добавлять в онтологию новые термины и отношения, которые необходимы для поддержки новых требований.

Уровень доверия к семантической сети определяется как вера в надёжность получаемых данных. Основными свойствами, определяющими уровень доверия к сети, являются: конфиденциальность, целостность и доступность данных. Текущий фокус исследований в контексте семантических сетей перекликается с надёжностью и достоверностью данных.

Оценку доверия в семантической сети можно выполнять, опираясь на централизованность и распределённость архитектурных решений. В централизованной системе информация, касающаяся деятельности каждого участника, собирается от других пользователей, которые имели непосредственный опыт работы с этим конкретным узлом в сети. Затем, в специальном модуле системы собираются все полученные рейтинги и подсчитываются баллы для каждого члена узла [20].

Что касается распределённой оценки репутации при принятии решений об обмене данными с другими участниками в сети, то здесь нет единого центра с рейтингами доверия, вместо этого есть несколько баз репутации, где каждый участник может обмениваться опытом взаимодействия с другими участниками сети [21].

При оценке доверия в распределенных системах как правило необходимо применять такие интеллектуальные средства, которые позволяют оценивать актуальные рейтинги для комментариев, предоставленных узлами, честность рекомендаций, предоставленных каждым узлом в семантических сетях, и оценка прошлого опыта работы с конкретным узлом, с которым предполагается взаимодействовать.

Заключение. При использовании семантических сетей сетевые ресурсы и службы должны быть защищены от несанкционированного доступа, а программные агенты должны быть уверены в конфиденциальности данных, которые они раскрывают службам. Широкий спектр связанных с безопасностью понятий, таких как аутентификация, авторизация, контроль доступа, конфиденциальность, целостность данных и приватность, имеют непосредственное отношение к семантическим сетям и требуют специального рассмотрения. Проблемы безопасности существуют в различных аспектах семантических сетей, и общую безопасность можно обеспечить, следуя определённому подходу или используя определённые механизмы. Для достижения этих целей были рассмотрены структуры семантических данных и информационных запросов к ним. В результате анализа выявлено, что было проделано не так много работ по созданию алгоритмов и стандартов для проверки достоверности и целостности данных.

В настоящее время низкоуровневое шифрование, механизмы цифровой подписи, сертификация и инфраструктура открытых ключей обеспечивают хорошую инфраструктуру безопасности. Однако обеспечение безопасности более высокого уровня, особенно без предварительных доверительных отношений, зависит от множества специальных механизмов, оставляет дыры в безопасности, требующие соответствующих разработок и исследований.

Как видно из изложенного аналитического материала в области защиты информации семантических сетей существует ряд не решённых проблем, связанных с отсутствием готовых рекомендаций по защите семантических сетей, которые достаточно актуальны и требуют эффективного решения на сегодняшний день. Создание эффективных средств защиты информации с использованием прежде всего современных криптографических методов является актуальной задачей. В дальнейшем, используя полученные результаты по специфике семантических сетей, планируется провести исследование потенциальных уязвимостей этой технологии, а также сформировать рекомендации для их решения с точки зрения информационной безопасности. Авторы статьи имеют результаты в области создания криптографических средств в не доверенных средах и могут применить эти результаты при построении средств защиты семантических сетей [22]. Необходимы дальнейшие исследования относительно того, какие методы криптографической защиты являются наиболее подходящими, учитывая специфику исследуемой области.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Halpin H.* Semantic Insecurity: Security and the Semantic Web. – Paris, France, 2017.
2. *Muhammad L.J., Garba E.J., Oye N.D., Wajiga G.M.* On the Problems of Knowledge Acquisition and Representation of Expert System for Diagnosis of Coronary Artery Disease (CAD) // International Journal of u- and e- Service, Science and Technology. – 2018. – Vol. 11, No. 3. – P. 49-58.
3. *Хабаров С.* Курс лекций по дисциплине «Представление знаний в информационных системах» доцента кафедры информационных систем и технологий. – СПбГЛТУ.
4. *Patel A., Jain S.* Formalism of Representing Knowledge // 6th International Conference on Smart Computing and Communications. – 2017.
5. *Кобринский Б.А.* Методология формализации знаний. – РНИМУ им. Н.И. Пирогова, 2020.
6. The World Wide Web Consortium (W3C). Query. – URL: https://www.w3.org/standards/semanticweb/query.
7. *Macina A.* SPARQL distributed query processing over linked data. – Université Côte d'Azur, 2019.
8. *GibbinsN.* Semantic Web in Depth. SPARQL Protocol and RDF Query Language // Electronics and Computer Science. – University of Southampton, 2014.
9. *Bamashmoos F., Holyer I., Tryfonas T., Woznowski P.* Towards Secure SPARQL Queries in Semantic Web Applications using PHP Faculty of Engineering. – University of Bristol, Bristol, United Kingdom Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. – 2017.
10. *Kirrane S., Villatam S., d'Aquin M.* Privacy, security and policies: A review of problems and solutions with semantic web technologies // Semantic Web. – 2018. – Vol. 9, No. 2. – P. 153-161.
11. *Rahimzadeh Holagh S., Mohebbi K.* A glimpse of Semantic Web trust // SN Applied Sciences. – Switzerland, 2019.
12. *Medi´c A., Golubovi´c A.* Making secure semantic Web // Universal Journal of Computer Science and Engineering Technology. – 2010. – P. 99-104.
13. *Fizza Abbas U., Hussain R., Son J., Oh H.* A Study of RDF Security Concerns in Semantic Web // Fall Conference of the Korean Society for Information Processing. – 2013. – Vol. 20, No. 2. – P. 906-909.
14. *Malik N., Kumar S. Malik* Security in Web Semantics: A Revisit // 12th INDIACom; INDIACom-2018; 5th International Conference on Computing for Sustainable Global Development. – 2018.
15. *Atkinson S., Jagodzinski P., Johnson C., Phippen A.* Semantic Web: a personal privacy perspective // WIT Transactions on Information and Communication Technologies. – 2006.
16. *Одиночкина С.В.* Основы технологий XML. – СПб.: НИУ ИТМО, 2013. – 56 с.
17. *Elnaggar A.* The Semantic Web. Department of Information Technology, Institute of Graduate Studies and Research, University of Alexandria, Egypt. – 2015.
18. *Sazonau, V., Sattler, U., Brown, G.* General Terminology Induction in OWL // The Semantic Web – ISWC 2015: 14th International Semantic Web Conference. – 2015. – P. 533-550.
19. *Maedche A., Volz R.* The ontology extraction & maintenance framework Text-To-Onto // Proceedings of the Workshop on Integrating Data Mining and Knowledge Management. – 2001.

20. *Glimm B., Stuckenschmidt H.* 15 Years of Semantic Web: An Incomplete Survey // Künstliche Intelligenz. – Springer, 2016. – Vol. 30, No. 2. – P. 117-130.
21. *Sabater J., Sierra C.* REGRET: a reputation model for gregarious societies // Proceedings of the 4th international workshop on deception, fraud and trust in agent societies. – 2005. – P. 61-69.
22. *Babenko L.K., Tolomanenko E.A.* Development of algorithms for data transmission in sensor networks based on fully homomorphic encryption using symmetric Kuznyechik algorithm // Journal of Physics: Conference Series. – 2021. – 1812. – 012034. – DOI: 10.1088/1742-6596/1812/1/012034.

REFERENCES

1. *Halpin H.* Semantic Insecurity: Security and the Semantic Web. Paris, France, 2017.
2. *Muhammad L.J., Garba E.J., Oye N.D., Wajiga G.M.* On the Problems of Knowledge Acquisition and Representation of Expert System for Diagnosis of Coronary Artery Disease (CAD), *International Journal of u- and e- Service, Science and Technology,* 2018, Vol. 11, No. 3, pp. 49-58.
3. *Khabarov S.* Kurs lektsiy po distsipline «Predstavlenie znaniy v informatsionnykh sistemakh» dotsenta kafedry informatsionnykh sistem i tekhnologiy [Course of lectures on the discipline "Knowledge Representation in Information Systems", Associate Professor of the Department of Information Systems and Technologies]. SPbGLTU.
4. *Patel A., Jain S.* Formalism of Representing Knowledge, *6th International Conference on Smart Computing and Communications*, 2017.
5. *Kobrinskiy B.A.* Metodologiya formalizatsii znaniy [Methodology of knowledge formalization]. RNIMU im. N.I. Pirogova, 2020.
6. The World Wide Web Consortium (W3C). Query. Available at: https://www.w3.org/standards/semanticweb/query.
7. *Macina A.* SPARQL distributed query processing over linked data. Université Côte d'Azur, 2019.
8. *GibbinsN.* Semantic Web in Depth. SPARQL Protocol and RDF Query Language, *Electronics and Computer Science*. University of Southampton, 2014.
9. *Bamashmoos F., Holyer I., Tryfonas T., Woznowski P.* Towards Secure SPARQL Queries in Semantic Web Applications using PHP Faculty of Engineering. University of Bristol, Bristol, United Kingdom Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia, 2017.
10. *Kirrane S., Villatam S., d'Aquin M.* Privacy, security and policies: A review of problems and solutions with semantic web technologies, *Semantic Web,* 2018, Vol. 9, No. 2, pp. 153-161.
11. *Rahimzadeh Holagh S., Mohebbi K.* A glimpse of Semantic Web trust, *SN Applied Sciences*. Switzerland, 2019.
12. *Medi´c A., Golubovi´c A.* Making secure semantic Web, *Universal Journal of Computer Science and Engineering Technology,* 2010, pp. 99-104.
13. *Fizza Abbas U., Hussain R., Son J., Oh H.* A Study of RDF Security Concerns in Semantic Web, *Fall Conference of the Korean Society for Information Processing,* 2013, Vol. 20, No. 2, pp. 906-909.
14. *Malik N., Kumar S. Malik* Security in Web Semantics: A Revisit, *12th INDIACom; INDIACom-2018; 5th International Conference on Computing for Sustainable Global Development,* 2018.
15. *Atkinson S., Jagodzinski P., Johnson C., Phippen A.* Semantic Web: a personal privacy perspective, *WIT Transactions on Information and Communication Technologies,* 2006.
16. *Odinochkina S.V.* Osnovy tekhnologiy XML [Fundamentals of XML technologies]. Saint Petersburg: NIU ITMO, 2013, 56 p.
17. *Elnaggar A.* The Semantic Web. Department of Information Technology, Institute of Graduate Studies and Research, University of Alexandria, Egypt, 2015.
18. *Sazonau, V., Sattler, U., Brown, G.* General Terminology Induction in OWL, *The Semantic Web – ISWC 2015: 14th International Semantic Web Conference*, 2015, pp. 533-550.
19. *Maedche A., Volz R.* The ontology extraction & maintenance framework Text-To-Onto, *Proceedings of the Workshop on Integrating Data Mining and Knowledge Management,* 2001.
20. *Glimm B., Stuckenschmidt H.* 15 Years of Semantic Web: An Incomplete Survey, *Künstliche Intelligenz*. Springer, 2016, Vol. 30, No. 2, pp. 117-130.

21. *Sabater J., Sierra C.* REGRET: a reputation model for gregarious societies, *Proceedings of the 4th international workshop on deception, fraud and trust in agent societies*, 2005, pp. 61-69.
22. *Babenko L.K., Tolomanenko E.A.* Development of algorithms for data transmission in sensor networks based on fully homomorphic encryption using symmetric Kuznyechik algorithm, *Journal of Physics: Conference Series*, 2021, 1812, 012034. DOI: 10.1088/1742-6596/1812/1/012034.

Статью рекомендовал к опубликованию д.т.н. Г.Е. Веселов.

Бабенко Людмила Клементьевна – Южный федеральный университет; e-mail: lkbabenko@sfedu.ru; г. Таганрог, Россия; тел.: 89054530191; кафедра безопасности информационных технологий; профессор.

Чудинов Павел Юрьевич – e-mail: chudinov@sfedu.com; тел.: 89198722200; кафедра безопасности информационных технологий; аспирант.

Рогозов Юрий Иванович – e-mail: yrogozov@sfedu.ru; тел.: +78634371787; кафедра системного анализа и телекоммуникаций; профессор.

Babenko Lyudmila Klimentevna – Southern Federal University; e-mail: blk@fib.tsure.ru; Taganrog, Russia; phone: +79054530191; the department of security of information technologies; professor.

Chudinov Pavel Yurevich – e-mail: chudinov@sfedu.ru.com; phone: +79198722200; the department of information technology security; postgraduate student.

Rogozov Yury Ivanovich – e-mail: yrogozov@sfedu.ru; phone: +78634371787; the department of system analysis and telecommunications; professor.

УДК 004.896 DOI 10.18522/2311-3103-2022-5-47-62

О.Б. Лебедев, А.А. Жиглатый

КО-ЭВОЛЮЦИОННЫЙ АЛГОРИТМ РАЗМЕЩЕНИЯ НА ОСНОВЕ ВЗАИМОДЕЙСТВИЯ СУБПОПУЛЯЦИЙ, ОТЛИЧАЮЩИХСЯ СТРАТЕГИЯМИ ПОИСКА*

Разработана новая методология и метод размещения элементов СБИС, отличающиеся тем, что решение задачи размещения основывается на использовании фиксированного порядка выбора позиций, ориентированного на эффективное решение задачи размещения, и эвристической процедуры распределения элементов по позициям, позволяющие снизить общую трудоемкость, и повысить качество решения. Процесс формирования списка позиций на коммутационном поле осуществляется с использованием механизмов волнового алгоритма. В основу выбора окончательного списка положен принцип построения маршрута с минимальной оценкой суммарной линейной длины расстояний между позициями маршрута. Для решения задачи размещения разработан поисковый алгоритм на основе модифицированного метода муравьиной колонии. Для исключения преждевременной сходимости и локализации глобального экстремума задачи разработка алгоритма производилась на основе ко-эволюционного подхода. Архитектура ко-эволюционного алгоритма размещения разработана на основе парадигмы муравьиного алгоритма. В пространстве поиска субпопуляции параллельно реализуют четыре стратегии оптимизации. В работе процесс ко-эволюции реализован на основе взаимодействия субпопуляций, отличающихся стратегиями поиска. Отличительной особенностью используемого ко-эволюционного подхода является то, что субпопуляции решений фактически являются виртуальными. Процесс ко-эволюции реализуется одной популяцией агентов Z путем последовательного формирования и слияния, виртуальных субпопуляций решений в одну популяцию. В работе решение задачи размещения направлено на повышение трассируемости посредством минимиз-

* Работа выполнена при финансовой поддержке гранта РФФИ № 20–07–00260 А.