имитационной модели: формализация имитационной модели, программирование имитационной модели и испытание имитационной модели.

Литература

1. Болдырев, В.В. Системный подход к разработке контура управления инновационного проекта создания интеллектуальной системы энергосбережения / В.В. Болдырев, М.А. Горькавый // Сборник научных трудов XVIII Международной научно-практической конференции, Санкт-Петербург, 2014. – С. 116-117.
2. Болдырев, В.В. Имитационная модель функционирования распределенной интеллектуальной системы энергосбережения с ограниченным количеством трудовых ресурсов/ В.В. Болдырев, М.А. Горькавый // Сборник научных трудов XIX Международной научно-практической конференции, – Санкт-Петербург, 2015. – С. 235–241.
3. Трусов Р.Е. Интеллектуальный модуль оценки эффективности работы команды инновационного проекта / Р.Е. Трусов, М.А. Горькавый // Современная наука: актуальные проблемы и пути их решения, Липецк, 2016. – С. 23-27.

УДК 004.652.3

ЗАЩИТА ИНФОРМАЦИИ В ОБЪЕКТНО-АТРИБУТНОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ[12]

Салибекян Сергей Михайлович, к.т.н., доцент Национального исследовательского университета «Высшая школа экономики», Московский институт электроники и математики, Москва, salibek@yandex.ru

В настоящее время развивается ОА-подход к организации структуры данных и вычислительного процесса. Данный подход реализует объектный принцип организации данных, однако данные имеют сетевую (графовую) структуру. Поэтому можно сказать, что ОА-структура данных относится к сетевому (графовому) типу базы данных (БД) [2], ОА-подход потребовал разработки новых методов защиты информации. Объектом защиты в ОА-системе является ОА-граф (база данных сетевого/графового типа). ОА-граф может содержать в себе не только информацию, но и программы (наподобие методов в объектно-ориентированной (ОО) парадигме). Сложность решения данной задачи состоит в том, что структура данных в ОА-БД может иметь любую топологию, а не только тип «дерева», как, например, в парадигме объектно-ориентированной (ОО). Объектом поиска в сетевой БД является либо одна запись, хранящаяся в узле графа, либо подграф. Поэтому для защиты информации в такой структуре не подойдут привычные методы, применяемые для реляционных баз данных [3] и ОО-БД [4].

Графовые БД развиваются достаточно динамично – появилось множество стандартов и программных продуктов, например: RDF, которая нашла достаточно широкое применение в Semantics Web, Neo4j [5] – сетевая БД, широко применяемая компаниями E-bay, Walmart, National Geographic, HP, CISCO и др. Графовая БД имеет неоспоримые преимущества перед реляционной в случае, когда необходимо работать со структурой данных, имеющей множество неструктурированных связей, и с данными, которые можно представить в виде диаграммы состояний переходов. Поэтому все это подтверждает актуальность данного научного направления, и вопросы защиты информации в графовых БД, в частности.

Теперь перечислим особенности ОА-принципа организации структуры данных, влияющие на принцип защиты информации. В вычислительной системе (ВС) в первую очередь требуется защищать от постороннего доступа информацию, которая может быть

[12] Статья рекомендована к опубликованию в журнале "Прикладная информатика"

считана или модифицирована несколькими пользователями. В ОА-ВС такой информацией является ОА-граф (БД графового типа). Сложность его защиты состоит в том, что он может иметь любую структуру, причем данные организованы динамически, т.е. связь между узлами графа осуществляется с помощью ссылок. Также сложность добавляет и то, что ОА-граф может подвергаться существенной модификации во время вычислительного процесса. Объектом поиска в ОА-графе может выступать как информационная капсула (ИК), так и подграф ОА-графа (в этом случае запросом будет являться ОА-граф).

По аналогии с другими БД защита ОА-графа может быть организована на уровне общего доступа (share-level security), когда ограничиваются права доступа ко всей БД (в нашем случае ОА-графу). Организация такой защиты не представляет собой сложности. Более интересен для нас уровень пользователя (User-level security), когда охраняются отдельные записи БД (в нашем случае ИК, ассоциированные с узлами ОА-графа). Для идентификации пользователей в данном случае могут применяться списки контроля доступа (Access Control List – ACL), куда заносятся сведения о правах пользователей на доступ к каким-либо полям БД (в нашем случае ИК или фрагментам ОА-графа). Хорошо зарекомендовала себя и модель безопасности, основанная на ролях (Role-based access control, RBAC), когда в ACL указываются права доступа не для конкретных пользователей, а для ролей – конкретный пользователь может быть связан с конкретной ролью. Такая модель безопасности существенно упрощает администрирование ВС.

User-level security в ОА-системе может быть организована на четырех уровнях: защита ОА-графа, защита фрагмента (подграфа) ОА-графа, защита ИК, защита информационной пары (ИП). Начнем с защиты ИК. В ИК находится множество ИП, которые описывают характеристики объекта или управление ФУ-ами (подпрограмма, аналогичная методу в ОО-парадигме). Защиту ИК можно осуществить двумя способами: «с помощью специальной ИП» и «с помощью указателя». В первом случае в ИК добавляется ИП с атрибутом «ACL» («Список контроля доступа»). Данная ИП используется только для контроля доступа к ИК: она игнорируется во время поиска информации в ИК и во время рассылки ИП, предназначенных для управления ФУ, и потому не влияет на работу ОА-ВС. Второй способ – добавление специального поля «указатель на список контроля доступа» («ACL location») в указатель на ИК. Например, в настоящее время указатель в программно реализованной экспериментальной ОА-системе имеет сложный формат: кроме непосредственно адреса ячейки памяти, в него входят поля: «тип данных», «индекс ИП», «индекс ИК», и этот список можно дополнить полем «указатель на таблицу прав доступа». Однако такое решение охраны ИК может привести к неоправданному расходу памяти ЭВМ, т.к., во-первых, не все ИК могут иметь защиту; во-вторых, указатели хранят адрес не только ИК, но и констант, и в этом случае дополнительное поле «ACL location» останется неиспользованным. Однако первый вариант защиты ИК также имеет недостатки: ФУ, осуществляющему контроль доступа, необходимо тратить время и вычислительные ресурсы на поиск защитной ИП в ИК. Однако, несмотря на недостатки, первый способ представляется нам наиболее приемлемым в ОА-ВС, т.к. он не требует дополнительной памяти во время решения вычислительных задач и обработки структур данных, не нуждающихся в защите информации.

Защиту на уровне фрагмента ОА-графа можно обеспечить двумя способами. Во-первых, поместив во все ИК фрагмента ОА-графа защитные ИП с указателем на единый ACL. Второй способ – поставить защиту ИК в так называемых точках входа в подграф. Точками входа могут быть, во-первых, внешние указатели (например, ссылка, передаваемая на ФУ, которое будет производить обработку ОА-графа), во-вторых, «мосты», связывающие фрагмент ОА-графа с основным ОА-графом (host-граф). Такой способ приемлем в том случае, когда обработка ОА-графа осуществляется с помощью его обхода. У данного способа есть один недостаток – ОА-граф может быть модифицирован в любой момент вычислительного процесса, и поэтому велика вероятность того, что в защите появится

«дырка» – внешняя ссылка или мост, который окажется незащищенным. Поэтому первый способ защиты фрагмента ОА-графа более предпочтителен, однако тот факт, что в каждой ИК находится защитная ИП, может привести к излишнему расходу памяти компьютера.

Защита всего ОА-графа может осуществляться тремя способами. Первый – единая ACL. Второй – защита по фрагментам, т.е. для каждого фрагмента существует своя ACL. Третий – защита внешних точек входа в ОА-граф (применимо только в случае обработка ОА-графа с помощью его обхода).

Защита на уровне ИП необходимо в том случае, когда пользователю необходимо предоставить не всю информацию из найденного в результате поиска ИП или фрагмента ОА-графа. Например, рядовому работнику можно предоставить список сотрудников, однако заблокировать все записи (в нашем случае ИП), где указывается зарплата работника. В реляционных БД эта проблем решается за счет того, что пользователю предоставляется доступ не к записи БД, а только к запросу, а запрос выводит пользователю лишь разрешенную информацию. В ОА-БД такую проблему можно решить, добавив в ACL поля «разрешенные атрибуты» и «запрещенные атрибуты», которые представляют собой список атрибутов ИП, информация из которых будет выдаваться (или не выдаваться) пользователю. Данные атрибуты учитываются ФУ, ответственным за выдачу результата поискового запроса. Например, для того, чтобы лишить пользователя возможности запускать на выполнение программы, встроенные в ОА-граф, необходимо добавить в список запрещенных атрибут Prog (в нагрузке ИП с таким атрибутом находится указатель на программу).

Для осуществления защиты информации выделим специализированное ФУ, называемое «Охранник» («Guard»). Данное ФУ осуществляет контроль учетных записей пользователей и ролей (если используется подход RBAC), а также создание и обработку ACL для ИК, входящих в состав ОА-графа. Ссылка на «охранника» помещается в контекст (совокупность внутренних регистров ФУ) рабочих ФУ (Work FU), которые осуществляют обработку ОА-графа. Такие ФУ прежде, чем приступать к обработке ИК ОА-графа, спрашивают «разрешение» на доступ к ней у «охранника», которому предварительно передается ссылка на эту ИК; если доступ запрещен, то «охранник» блокирует обработку ИК рабочим ФУ. На рис. 1 представлена схема функционирования системы контроля доступа к ОА-ВС.

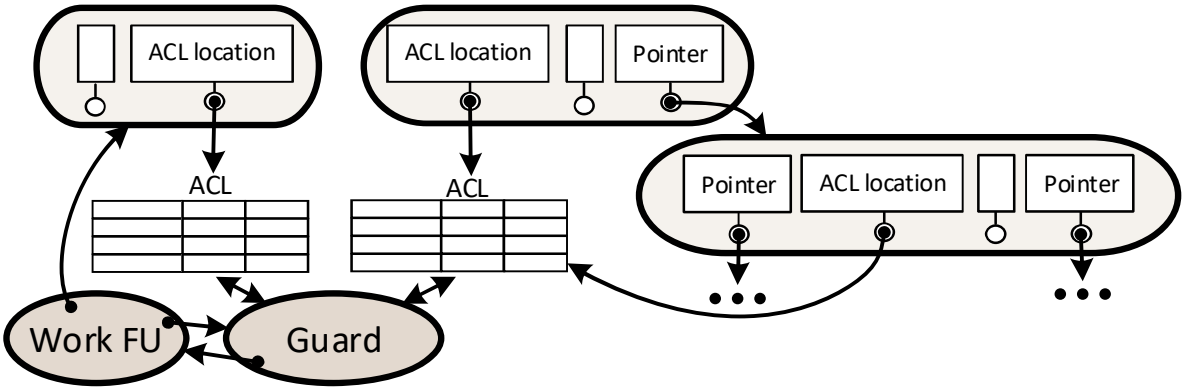

Рис. 1 – Механизм защиты информации в ОА-вычислительной системе

Для предотвращения несанкционированного доступа к ACL, адрес которой помещается в нагрузке защитной ИП, в алгоритм функционирования рабочего ФУ добавляются ограничения манипуляций с защитной ИП: запрет удаления защитной ИП (эта ИП может удаляться только во время удаления всей ИК, где она находится), запрет перехода по ссылке в нагрузке защитной ИП и т.д. Обработка таблиц прав доступа (создание, уничтожение и модификация) возлагается только на «охранника».

Предложенная методика работы защиты в ОА-ВС удобна тем, что позволяет копировать права доступа при копировании фрагмента ОА-графа. Этот механизм заменяет принцип наследования в ОО-парадигме: вместо копирования класса и добавления в него новых полей и методов используется копирование эталонного ОА-графа и дополнение его новыми вершинами и связями [2]. Находящиеся в ИК шаблона защитные ИП копируются вместе с другими ИП ОА-графа и адрес в нагрузке защитной ИП копируется без изменений: если ссылка в нагрузке ИП указывает на ячейку памяти, не относящуюся к ОА-графу, то при копировании ИП она не изменяется. Таким образом, все настройки защиты переносятся в копию фрагмента ОА-графа (рис. 2).

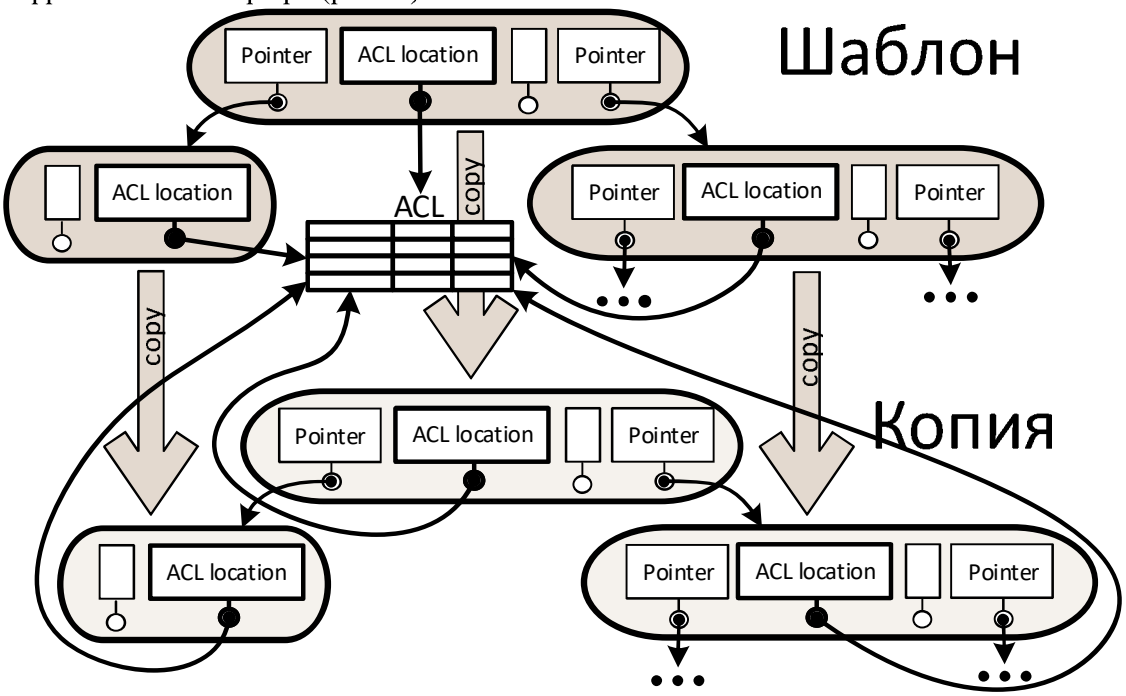

Рис. 2 – Копирование прав доступа при копировании фрагмента ОА-графа

Предложенная методика защиты в ОА-ВС обеспечивает защиту на всех уровнях ОА-ВС: ОА-графа, фрагмента ОА-графа, ИК и ИП. И хотя методика разработана специально для ОА-БД, она с некоторой модификацией, скорее всего, может быть использована для защиты других видов графовых БД.

Литература

1. Салибекян С.М., Панфилов П.Б. Объектно-атрибутная архитектура – новый подход к созданию объектных систем // Информационные технологии. 2012, №2 стр. 8-14
2. Салибекян С.М., Белоусов А.Ю. Сетевая база данных, построенная по объектно-атрибутному принципу. // Объектные системы – 2014 (зимняя сессия): материал IX Международной научно-практической конференции (Ростов-на-Дону, 10-12 мая 2014 г.) / Под общ. ред. П.П. Олейника. – Ростов-на-Дону: ШИ (ф) ЮРГТУ (НПИ) им. М.И. Платова, 2014. с. 70-76 URL: http://objectsystems.ru/files/2014WS/Object_Systems_2014_Winter_session_Proceedings.pdf
3. Райордан Р. Основы реляционных баз данных/Пер, с англ. — М.: Издательско-торговый дом «Русская Редакция», 2001. — 384 с.
4. Олейник П.П. Модель разграничения прав доступа в объектно-ориентированных приложениях // Проблемы информационной безопасности. Компьютерные системы. 2015. № 4. с. 70-78.
5. Aleksa Vukotic, Jonas Partner, Nicki Watt. Neo4j in Action. — Manning Publications Company, 2014.