УДК 004.056
DOI 10.53403/9785951505200_146

РЕАЛИЗАЦИЯ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА В СУБД POSTGRESQL ДЛЯ ЗАЩИЩЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ «АРАМИД»

Симаков Виталий Юрьевич (*vyusimakov@vniief.ru*), *Липов Денис Игоревич*, *Пищулин Игорь Анатольевич*

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

В докладе представлены функциональные возможности разработанных средств защиты информации, мандатная модель разграничения доступа защищенной операционной системы (ЗОС) «Арамид» и иерархия маркируемых объектов системы управления базами данных (СУБД).

Ключевые слова: Защищенная операционная система «Арамид», СУБД PostgreSQL, мандатный контроль доступа, модель Белла-ЛаПадулы, мандатный контекст.

IMPLEMENTATION OF MANDATORY ACCESS CONTROL IN THE POSTGRESQL DBMS FOR THE SECURE OPERATING SYSTEM «ARAMID»

Simakov Vitaly Yurievich (*vyusimakov@vniief.ru*), *Lipov Denis Igorevich*, *Pishilin Igor Anatolievich*

FSUE «RFNC-VNIIEF», Sarov Nizhny Novgorod region

The paper presents the functionality of the developed information security tools, the mandatory access control model of the secure operating system (SOS) «Aramid» and the hierarchy of the DBMS mandatory tags.

Key words: The secure operating system «Aramid», PostgreSQL DBMS, mandatory access control, Bell-LaPadula model, mandatory context.

Введение

Дистрибутив ЗОС «Арамид», ориентирован на создание автоматизированных систем в защищенном исполнении для проведения параллельных высокопроизводительных вычислений на супер-ЭВМ, в которых обрабатывается информация ограниченного распространения, в том числе содержащая сведения, составляющие государственную тайну со степенью секретности до «совершенно секретно» включительно [1].

Одним из важных компонентов данной ОС является СУБД, которая предназначена для накопления, обработки и хранения, как пользовательской информации, так и информации возникающей в процессе эксплуатации вычислительных комплексов. При этом в соответствии с требованиями нормативных документов ФСТЭК России, к защищенным операционным системам, пользовательские данные необходимо хранить и обрабатывать с учетом степени секретности данной информации [2]. Таким образом, в рамках работ по созданию ЗОС «Арамид», реализация СУБД с поддержкой системы мандатного разграничения доступа [3] является стратегически важной задачей. Для этого в ЗОС «Арамид» была интегрирована СУБД PostgreSQL, в которую к имеющимся средствам защиты информации встроены средства защиты, обеспечивающие поддержку системы мандатного разграничения доступа и регистрацию событий безопасности.

Существующие СУБД

СУБД – комплекс языковых и программных средств, позволяющих создать базу данных (БД) и манипулировать данными (добавлять, обновлять, удалять и выбирать). Система обеспечивает безопасность, надежность хранения и целостность данных, а также предоставляет средства для администрирования БД.

В настоящее время существует большое количество СУБД, как коммерческих, так и распространяющихся с открытыми исходными кодами. Ниже приведен анализ наиболее популярных из них.

MySQL – одна из самых популярных баз данных для веб-приложений. Разработку и поддержку MySQL осуществляет корпорация Oracle. Продукт распространяется как под лицензией GNU, так и под собственной коммерческой лицензией. Несмотря на то, что продукт предлагает много функций, даже в бесплатной версии, для коммерческого использования необходима покупка лицензии.

MariaDB – ответвление от системы управления базами данных MySQL. СУБД является бесплатной, но предлагает и платные версии. Она полностью совместима с MySQL, и подходит в качестве замены, однако, на данный момент стабильность ниже, чем у MySQL.

Oracle Database – объектно-реляционная система управления базами данных компании Oracle. СУБД является крайне надежной, фактически это эталон надежности среди подобных систем, но продукт является полностью коммерческим.

ЛИНТЕР – российская СУБД, реализующая стандарт SQL: 2003. Рекомендована «Единым реестром российских программ». Однако имеет коммерческую лицензию и низкую эффективность в случае высокой динамики изменений данных.

MongoDB – система управления базами данных с открытым исходным кодом. Классифицируется как NoSQL СУБД, т. е. SQL не используется в качестве языка запросов.

Microsoft SQL сервер – популярная СУБД, имеющая хорошую интеграцию с другими продуктами Microsoft. Однако лицензия имеет неприемлемую для большей части юридических лиц и организаций стоимость.

PostgreSQL – активно развивающаяся реляционная СУБД с открытым исходным кодом, поддерживает возможности стандарта SQL и предлагает множество современных функций:

- сложные запросы;
- внешние ключи;
- триггеры;
- изменяемые представления;
- транзакционная целостность.

Благодаря свободной лицензии, разрешается бесплатно использовать, изменять и распространять PostgreSQL для любых целей – личных, коммерческих или учебных.

В связи с вышесказанным в качестве базовой СУБД для реализации мандатного разграничения доступа в ЗОС «Арамид» была выбрана PostgreSQL.

Система мандатного разграничения доступа ЗОС «Арамид»

Мандатный контроль доступа – контроль доступа, основанный на мандатном разграничении доступа (Mandatory Access Control, MAC), которое определяется четырьмя условиями:

- все субъекты и объекты системы однозначно идентифицированы;
- задана решетка уровней конфиденциальности информации. Такая решетка определяет иерархию уровней секретности информации (например, «Несекретно», «Секретно», «Совершенно секретно»), а также место каждого объекта системы в данной иерархии;
- каждому объекту системы присвоен уровень конфиденциальности, определяющий ценность содержащейся в нем информации;
- каждому субъекту системы присвоен уровень доступа, определяющий уровень доверия к нему в компьютерной системе.

Основная цель мандатного разграничения доступа – предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа, т. е. противодействие возникновению в компьютерной системе неблагоприятных информационных потоков сверху вниз.

В качестве модели защиты в ЗОС «Арамид» используется встроенная в ОС дискреционная модель доступа и мандатная модель, построенная на основе модели Белла-ЛаПадулы [4] с возможностью модификации режимов мандатного доступа. В рамках модели Белла-ЛаПадулы, каждому субъекту и каждому объекту в системе приписывается специальный атрибут – уровень секретности. На рис. 1 приведена логика работы базовой модели Белла-ЛаПадулы.

Рис. 1. Базовая модель Белла-ЛаПадулы

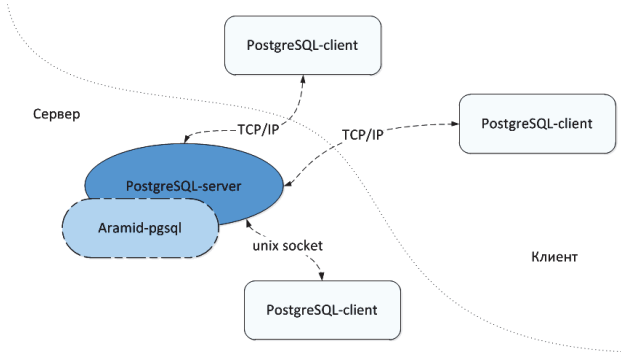

Рис. 2. Схема взаимодействия компонент СУБД PostgreSQL

Схема взаимодействия компонент СУБД PostgreSQL

СУБД PostgreSQL реализована в архитектуре клиент-сервер [5]. Рабочий сеанс PostgreSQL включает следующие взаимодействующие процессы (программы):

- главный серверный процесс, управляющий файлами баз данных и выполняющий различные запросы клиентов к базам данных;
- клиентское приложение пользователя, отправляющие запросы на выполнение операций в базе данных.

Сервер PostgreSQL может обслуживать одновременно несколько подключений клиентов. Он выполняет обработку запросов на соединение, а также аутентификацию клиентов, после чего запускает серверные процессы для каждого клиента, успешно прошедшего аутентификацию. Схема взаимодействия компонент СУБД PostgreSQL с поддержкой мандатного разграничения доступа ЗОС «Арамид» отображена на рис. 2.

Aramid-pgsql – компонент реализующий поддержку мандатного разграничения доступа ЗОС «Арамид». Средства защиты информации используют механизмы назначения, хранения, и модификации мандатных меток пользователей, предоставляемые операционной системой. Субъектом доступа является пользовательская сессия. Мандатный контекст сессии совпадает с мандатной меткой соединения с СУБД, получаемой для каждой сессии отдельно. В дальнейшем полученный контекст используется во всех запросах пользователя к защищаемым объектам БД. Иными словами, уровень доступа пользователя в СУБД определяется уровнем конфиденциальности, под которым пользователь работает в ОС. Защищаемыми объектами являются строки, столбцы, таблицы, представления, функции, схемы и базы данных.

Мандатная метка объекта БД имеет структуру мандатной метки ЗОС «Арамид»:

- иерархическая часть (Уровень);
- неиерархическая часть (Категория);
- атрибут:
  - 0×0 – мандатная метка дочерних объектов должна быть равна мандатной метке родительского объекта;
  - 0×1 – дочерние объекты могут иметь метку отличную от метки родительского объекта;
  - 0×2 – данный тип атрибута используется для работы с доверенными процедурами.

Мандатная метка создаваемого объекта БД назначается автоматически и всегда равна мандатной метке клиента, который выполняет запрос. В дальнейшем только администратор СУБД может изменить мандатную метку объекта БД.

Проверка мандатных прав доступа к объектам базы данных осуществляется совместно с дискреционными правами. Таким образом, доступ предоставляется только при санкционировании дискреционными и мандатными правилами разграничения доступа.

Доверенные процедуры/функции

В PostgreSQL с поддержкой мандатного разграничения доступа ЗОС «Арамид» реализована возможность запускать доверенный код с меткой безопасности, отличной от метки клиента. Данная функция используется для предоставления четко контролируемого доступа к важным данным (при этом, например, могут отсеиваться строки или хранимые значения могут выводиться с меньшей точностью). Будет ли функция вызываться как доверенная процедура, определяется ее мандатной меткой. Сделать функцию доверенной может только администратор СУБД.

На рис. 3 приведен пример использования доверенных процедур: Пользователь с мандатным контекстом «1:0×1» осуществляет чтение данных из таблицы «account_info», один из столбцов которой имеет мандатную метку «2:0×1». Операция завершается с ошибкой «security policy violation», т. к. мандатная метка столбца «card_num» выше мандатного контекста сессии. Пользователь не может обращаться к «card_num» напрямую, но доверенная процедура «get_card_num» позволяет ему получить номера кредитных карт клиентов, в которых будут скрыты некоторые цифры. Далее пользователь повторяет запрос, но для чтения данных из столбца «card_num» используется доверенная процедура «get_card_num». Данные успешно прочитаны, однако информация в столбце «card_num» отображена в измененном виде.

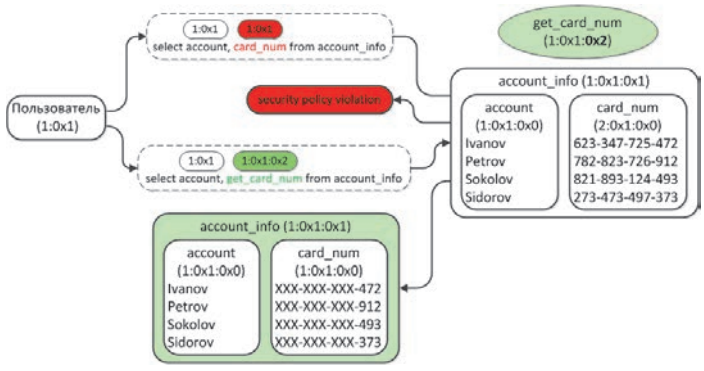

Рис. 3. Пример использования доверенных процедур

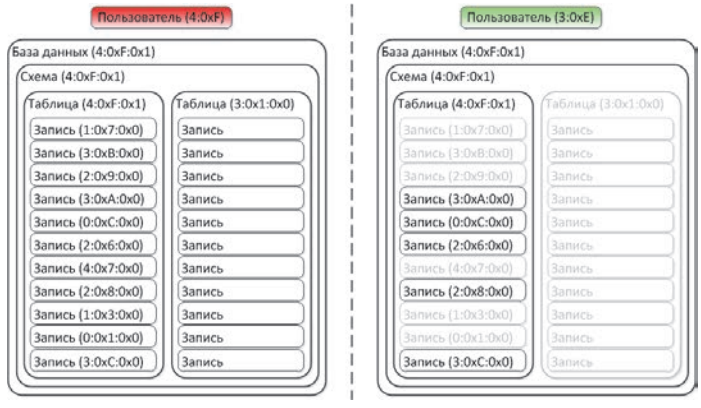

Рис. 4. Пример доступа к данным

Защита на уровне строк

Политика защиты строк ограничивает для пользователей наборы строк, которые могут быть возвращены обычными запросами или добавлены, изменены и удалены командами, изменяющими данные.

Выборка строк осуществляется на основе мандатного контекста пользователя и мандатной метки строки, к которой осуществляется доступ:

- SELECT – строка выводится пользователю, когда мандатный контекст пользователя больше или равен мандатной метки строки;
- INSERT – разрешено, если мандатный контекст пользователя равен мандатной метке строки;
- UPDATE/DELETE – редактирование строки разрешено, когда мандатная метка строки равна мандатному контексту пользователя.

Мандатная метка строки имеет структуру мандатной метки ЗОС «Арамид» и хранится в специальном столбце таблицы: «aramid_label».

На рис. 4 приведен пример чтения данных пользователями с разными мандатными контекстами. Все данные, имеющиеся в БД, имеют мандатную метку меньшую, чем у пользователя с мандатным контекстом «4:0×F», поэтому он может прочитать их все. Пользователю с мандатным контекстом «3:0×E», из этой же БД может прочитать только ту информацию, мандатная метка которой меньше или равна его уровня доступа.

Заключение

СУБД PostgreSQL с поддержкой системы мандатного разграничения доступа ЗОС «Арамид» позволяет организовать хранение и обработку различной информации со степенью секретности до «совершенно секретно» включительно.

Доработанные средства аудита обеспечивают регистрацию следующих событий безопасности:

- идентификация и аутентификация пользователей;
- запрос на доступ к защищаемому объекту;
- создание, удаление и изменение объектов СУБД.

Список литературы

1. Петрик А. Н. Защищенная операционная система «Арамид» для супер-ЭВМ. Сборник тезисов Национального суперкомпьютерного форума (НСКФ-2019), 2019.

2. Требования безопасности информации к операционным системам. ФСТЭК России, 2016.

3. Цирлов В. Л. Основы информационной безопасности автоматизированных систем. Феникс, 2008.

4. Bell D. E., LaPadula L. J. Secure Computer Systems: Unified Exposition and Multics Interpretation: Technical Report ESD-TR-75-306. The MITRE Corporation. Bedford: MA, 1975.

5. Документация к PostgreSQL 11 [Электронный ресурс] – URL: https://postgrespro.ru/media/docs/postgresql/11/ru/postgres-A4.pdf.