Модель системы ролевого доступа

Рогачева А.В.
alinarogacheva@mail.ru
Балашовский институт Саратовского государственного университета имени Н.Г. Чернышевского

В статье рассматриваются вопросы, связанные с изучением ролевого управления доступом посредством объектно-ориентированного моделирования, с целью повышения качества учебного процесса. При анализе предметной области структура системы ролевого управления доступом описывается наглядно с помощью UML-диаграмм.

Ключевые слова: информационная безопасность, управление доступом, ролевое управление, моделирование, UML.

Владение информационным моделированием как основным методом приобретения знаний является одним из основных метапредметных результатов, формируемым при изучении информатики в школе. Через призму моделирования информатика рассматривает объекты и процессы, которые относятся к различным областям знаний. При этом особую роль моделирование играет при изучении понятий, которые входят в предметную область информатики. Такой подход позволяет более наглядно объяснить те или иные процессы и закономерности. Объектно-ориентированное моделирование помогает структурировать исследуемую область с высокой степенью точности и наглядности. Вопросы, которые касаются изучения информационной безопасности, тоже логично интерпретируются объектными моделями [1]. Объектно-ориентированный подход в информационной безопасности позволяет упростить описание многих сущностей и процессов, сопровождая их наглядными UML-диаграммами [2]. Такой подход позволяет, в целом, повысить качество учебного процесса.

Рассмотрим проблему моделирования системы ролевого доступа. На сегодняшний день она является наиболее популярной моделью логического управления доступом. В ней между пользователями и их правами доступа появляются промежуточные сущности – роли. Главными преимуществами использования ролевой системы контроля доступа в крупных многопользовательских системах хранение информационных ресурсов являются простота администрирования и возможность разделения обязанностей [3].

Ролевая политика подразумевает осуществление контроля доступа администратором в две стадии:

- каждой роли сопоставляется набор полномочий;
- для каждого пользователя составляется список доступных ему ролей.
- Система ролевого доступа должна предусматривать:
- добавление пользователей и назначение их на роль;
- определение и хранение прав ролей;
- хранение информации о принадлежности ролей пользователям.

Эти функции системы описаны подробнее с помощью UML-диаграмм.

Рассмотрим диаграмму вариантов использования системы управления доступом на основе ролей, представленную на рисунке 1. В качестве актёров на диаграмме представлены пользователь и администратор системы.

Главное место в процессе управления доступом занимает администратор системы. Для актера «Администратор» представлены следующие варианты использования:

«Зарегистрировать нового пользователя» – Администратор вводит данные нового пользователя в таблицу «Пользователь».

«Предоставить роль пользователю» – администратор выбирает пользователя и сопоставляет ему существующую роль, при этом соответствующая запись заносится в таблицу «Назначение роли пользователя».

«Назначить разрешение роли» – существующей роли предоставляется право на действие над объектом, при этом сопоставляются записи соответствующих трех таблиц, новая запись заносится в таблицу «Назначение прав роли».

Для актёра «Пользователь» определены варианты использования «Войти в систему», «Просмотреть список доступных объектов» и «Выполнить операцию над объектом».

Кроме занесения сведений в базу данных, для подсистемы ролевого доступа представлены варианты использований: «Проверить разрешение на операцию» и «Зарегистрировать операцию», которые задействуются при выполнении пользователем прецедента «Выполнить доступную операцию над объектом».

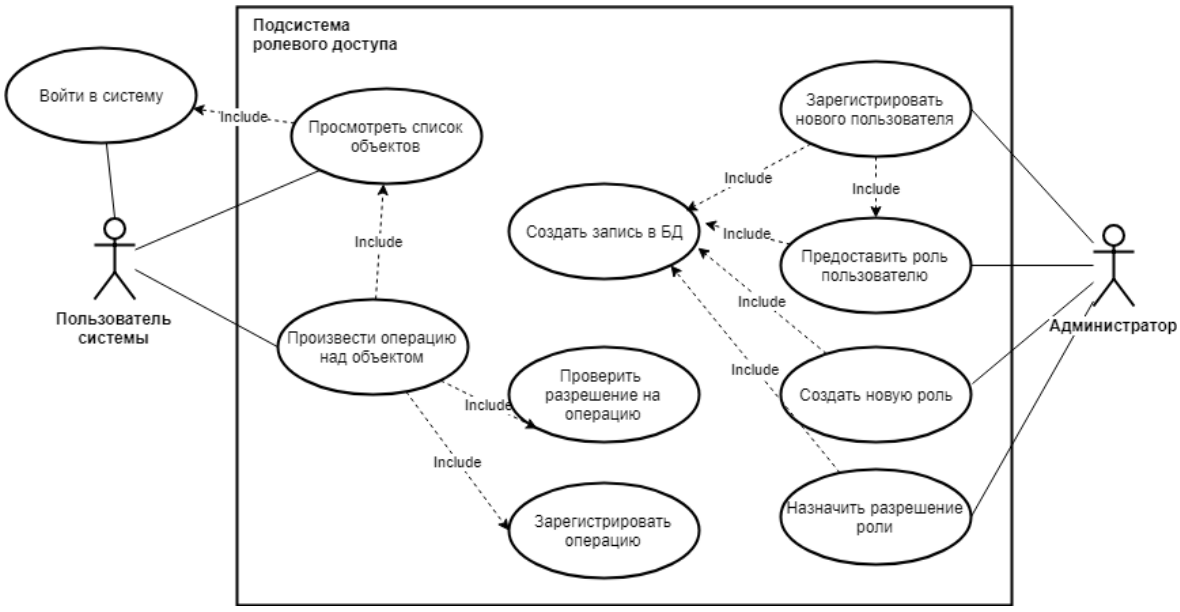

Рис. 1. Диаграмма вариантов использования

Структура базы данных системы ролевого доступа отражена на диаграмме на рисунке 2. Основными являются таблицы «Пользователь», «Роль», «Операция» и «Объект», каждая из которых имеет по одному ключевому элементу, идентифицирующих записи – первичному ключу.

Помимо ключевого поля, таблица «Объект» имеет поля для указания

названия и типа объекта; таблицы «Операция» и «Роль» имеют поле «Название»; таблица «Пользователь» содержит поля для хранения данных для авторизации пользователей в системе.

Системой подразумевается возможность пользователя иметь несколько ролей, и, в свою очередь, одна роль подразумевает включение многих пользователей. Связь «многие-ко-многим» осуществлена посредством связывающей таблицы «Назначение роли пользователя». Аналогично таблицы «Объект», «Операция» и «Роль» связаны таблицей «Назначение прав роли». При этом все таблицы на рисунке соединены связью «один-ко-многим». Связывающие таблицы имеют только внешние ключи – идентификаторы записей соответствующих таблиц.

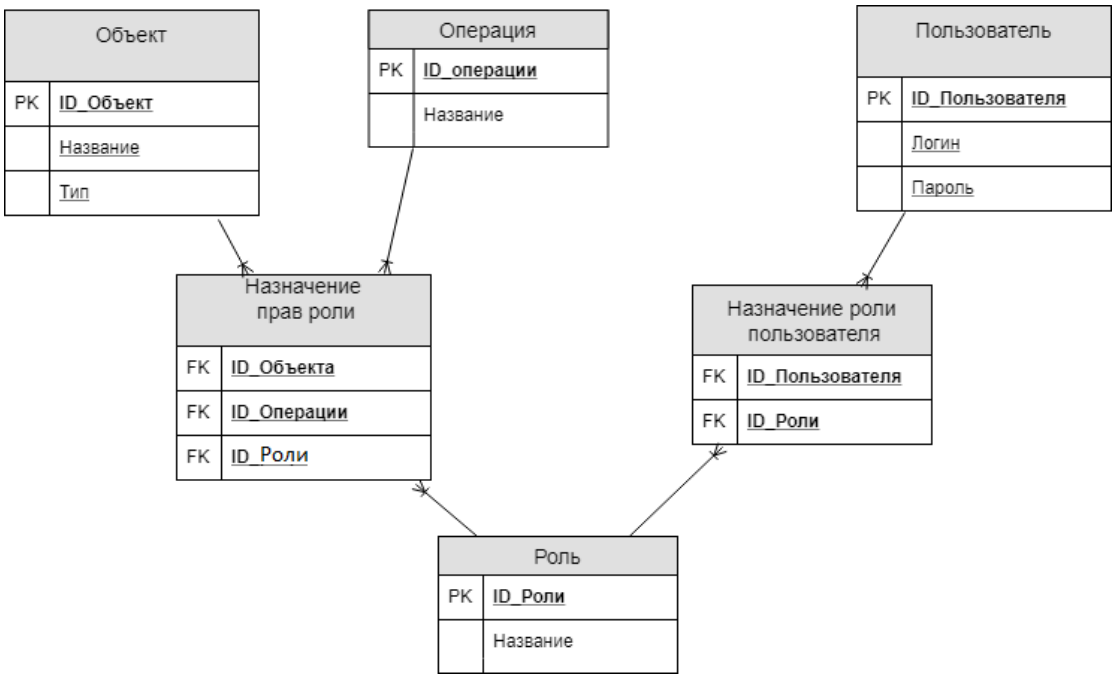

Рис. 2. Структурная модель базы данных

Основной функцией в администрировании системы является сопоставление набора полномочий существующей роли. Последовательность действий предоставления права роли представлена на рисунке 3.

В процессе назначения права актером «Администратор» задействуются сразу таблицы «Объект», «Операция», «Роль». Запись, фиксирующая назначение разрешений вносится в таблицу «Назначение прав роли».

Алгоритм действий администратора и системы приведен на рисунке 4.

Диаграмма деятельности показывает алгоритм всех осуществляемых действий в ходе назначения права роли. Администратор выбирает роль, которой должен назначить разрешение, объект доступа и производимое над ним действие. После этого системой проводится проверка условия: предоставлено ли такое разрешение ранее. Если роли еще не сопоставлено данное действие на выбранный объект, то вносится соответствующая запись в таблицу «Назначение прав роли».

Разработанная модель помогает объяснить и проиллюстрировать особенности ролевого разграничения доступа. Например, возможность

реализовать гибкие, изменяющиеся динамически в процессе функционирования компьютерной системы, правила разграничения доступа. Такое разграничение доступа является составляющей многих современных компьютерных систем.

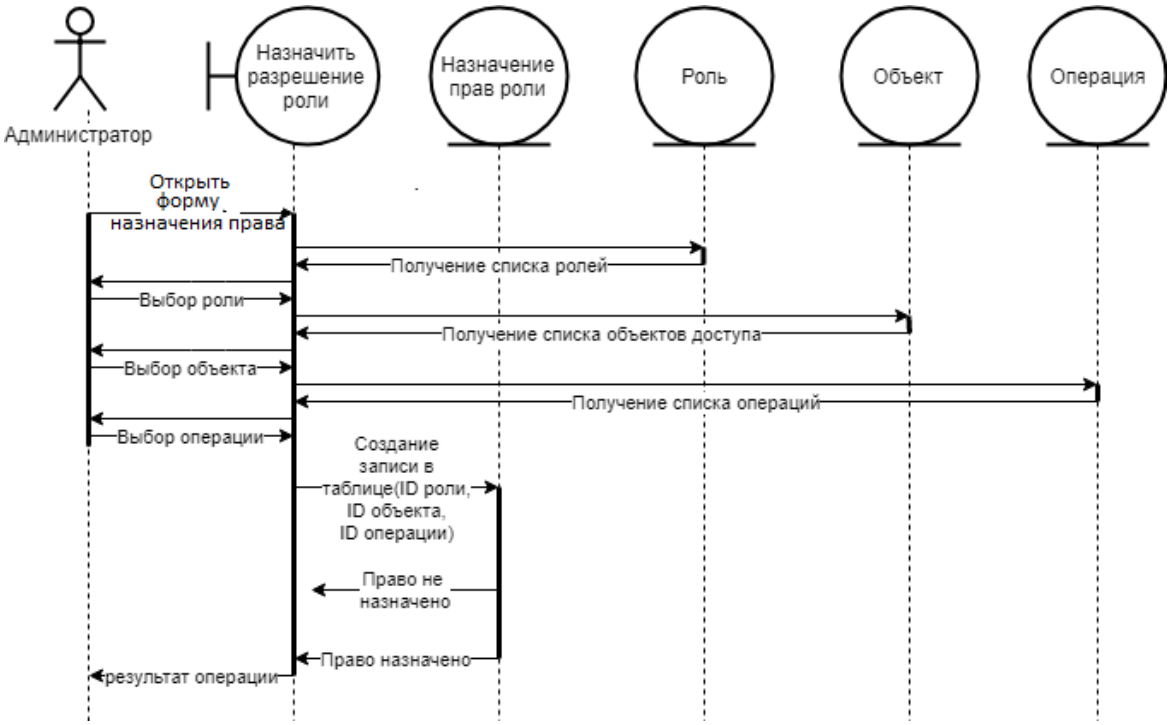

Рис. 3. Диаграмма последовательности действий по прецеденту «Назначить разрешение роли»

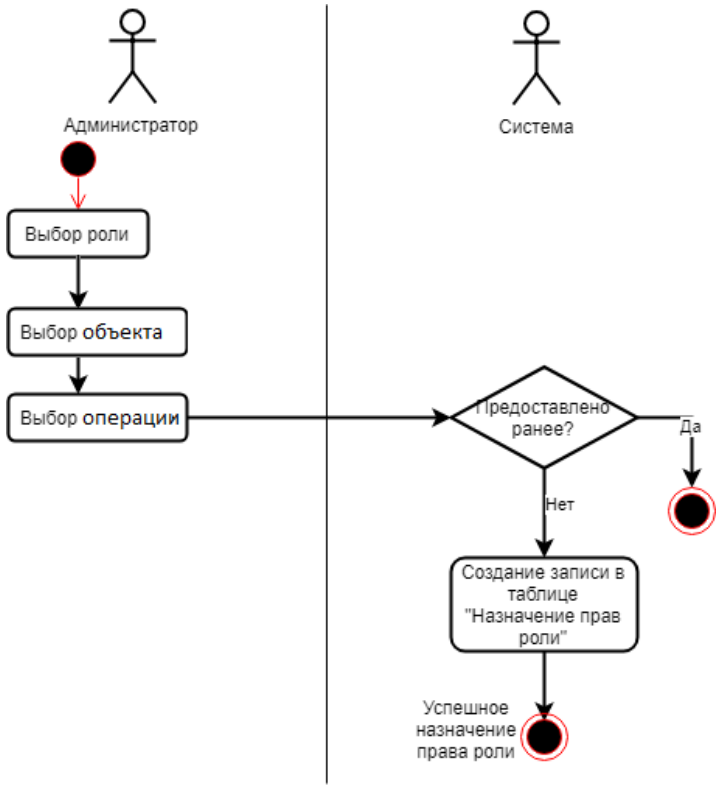

Рис. 4. Диаграмма деятельности для прецедента «Назначить разрешение роли»

Как правило, данный подход применяется в системах защиты СУБД, а отдельные элементы реализуются в сетевых операционных системах[4]. Отдельно следует отметить, что на основании рассмотренной модели может быть разработана и реальная система, которая позволит организовать механизм управления доступом на основе ролей.

Список литературы

[1] *Грибанова-Подкина М.Ю.* Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования // Вопросы безопасности. 2017. № 2. С.25-34. DOI: 10.7256/2409-7543.2017.2.22065. URL: http://e-notabene.ru/nb/article_22065.html

[2] *Грибанова-Подкина М.Ю.* Использование объектно-ориентированного подхода в изучении информационной безопасности при подготовке педагогических кадров // Научно-методические проблемы инновационного педагогического образования: Сб. науч. тр.: В 2 ч. Ч.1. – Саратов: Изд-во СРОО «Центр «Просвещение», 2017. – С. 91-94.

[3] *Малюк, А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации. //М.: ГЛТ, 2012. – 280 с.

[4] *Васельков, А. В.* Безопасность и управление доступом в информационных системах // М.: Форум, 2013. – 368 с.