

Формальное представление моделей систем безопасности

Владиминова Т.Л., Пилько С.В.

Белорусский национальный технический университет

Рассматривается методологическая основа для концептуального описания моделируемых объектов систем безопасности, в том числе систем контроля и управления доступом.

В силу своей специфики, системы контроля доступа являются системами реального времени (СРВ).

СРВ, как аппаратно-программный комплекс включает в себя датчики, регистрирующие события на объекте, модули ввода-вывода, преобразующие показания датчиков в цифровой вид, пригодный для обработки этих показаний на компьютере и компьютер с программой, которая реагирует на события происходящие на объекте. Ее основная задача - реагировать в предсказуемые времена на непредсказуемый поток внешних событий. Это означает, что система должна отреагировать на событие произошедшее на объекте своевременно, т. е. в течение времени критического для данного события. Величина критического времени для каждого события определяется объектом и самим событием, и, естественно может быть разной, но время реакции системы должно быть предсказано (вычислено при создании системы. Отсутствие реакции в предсказанное время считается ошибкой для систем реального времени. Кроме этого система должна успевать реагировать на одновременно происходящие события. Даже если два или большее число внешних событий происходят одновременно, система должна успеть среагировать на каждое из них в течение временных интервалов, критических для этих событий.

Различают системы реального времени двух типов: системы жесткого реального времени и системы мягкого реального времени. Системы жесткого реального времени не допускают никаких задержек реакции системы так как результаты могут быть бесполезными в случае опоздания, может произойти нарушение действий системы в случае задержки реакции, стоимость опоздания может оказаться бесконечно велика. Системы мягкого реального времени характеризуются тем, что задержка

реакции допустима, хотя и может привести к увеличению стоимости системы. СКУД относятся именно к этому типу систем.

Понимание системы контроля доступа как системы реально-го времени требует использования ряда специфических механизмов, оказывающих существенное влияние на архитектуру всей системы, а значит и на ее формальное представление.

На сегодняшний день для написания программ часто используется объектно-ориентированный подход, позволяющий разработчику абстрагироваться от алгоритма как последовательности указаний.

Для дальнейшего увеличения эффективности требуется специальные средства, которые помогут продумать и промоделировать систему, избежать фатальных ошибок. Нужны средства, которые позволят визуально изобразить объекты и их взаимодействия, нужны методики, которые позволят последовательно найти и изучить взаимодействующие объекты, продумать процесс разработки и адаптировать его к изменяющимся потребностям.

СКУД, ориентированные на обслуживание большого числа клиентов, обычно имеют модульную структуру, позволяющую организовать рабочие места для различных служб, которые обеспечивают эффективное функционирование системы. Модульная схема обеспечивается за счет архитектуры клиент-сервер. Для небольших систем, где роль обслуживающего персонала играет только один человек вся необходимая функциональность может быть сведена в единый модуль.

В качестве среды взаимодействия служебных приложений и сервера СКУД могут выступать локальная вычислительная сеть или адресное пространство одного компьютера.

Модель предметной области представлена на рис.1. Группа представляет собой любое объединение людей (сотрудники подразделения, посетители). Каждый человек в системе обязательно приписан какой-либо группе. Доступ пользователей в свои зоны доступа осуществляется с помощью идентификатора доступа имеющего код, который является практически паролем доступа. Когда в систему должен быть добавлен новый пользователь, для него либо добавляется группа, если таковой в системе не существует, либо он вносится в список уже существующей группы.

В системе имеется администратор, который имеет право добавить нового пользователя, добавить новую группу, настраивать права и расписание прав доступа членов каждой группы, устанавливать ассоциации внутри каждой группы и между группами.

Для того, чтобы человек мог пользоваться системой ему выдается карта. На каждую учетную запись может быть выдана только одна карта. Несколько учетных записей не могут использовать одну карту.

Для того чтобы построить иерархию групп между ними можно устанавливать связи. Группа, установившая связь, решает использовать свои права для установления ассоциации между ними.

Каждая зона (ресурс) связана с некоторым действием. С другой стороны, группой могут быть присвоены различные права на выполнение действий в зоне.

В зависимости от типа контроллера турникета у него может быть несколько направлений действия. Каждое направление связано с двумя зонами (зона откуда осуществляется доступ и зона куда осуществляется доступ)

В зависимости от назначения помещения у контроллера замка (защелки) может быть также несколько направлений действия. В одних каждое направление может быть связано с двумя зонами, как и у контроллера турникета, а в других с одной зоной (зона куда осуществляется доступ).

Трафик СКУД как системы реального времени требует реализации механизма диспетчеризации, меж объектового взаимодействия и средств работы с таймерами. Параллелизм в обработке одновременно происходящих внешних событий должен обеспечиваться за счет использования многопоточности. Клиент серверный подход вносит необходимость реализации механизма и способов взаимодействия между сервером и приложениями, а общие требования безопасности и надежности заставляют выбирать особые способы хранения данных и работы с ними.

