ПРОЕКТИРОВАНИЕ СИСТЕМЫ КОНТРОЛЯ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ СТАНДАРТОВ СЕРИИ ИСО/МЭК 27000

П. Е. Ковалец

Стандартизация в области информационной безопасности (ИБ) позволяет установить оптимальный уровень упорядочения и унификации, подтвердить соответствие информационных систем предъявляемым к ИБ требованиям.

Однако сам процесс стандартизации зачастую требует значительных затрат, как финансовых, так и временных. Таким образом, актуально

проектирование системы контроля реализации в организации требований стандартов ИБ с целью уменьшения затрат на прохождение процедуры сертификации.

В качестве конкретного семейства стандартов была выбрана серия международных стандартов ИСО/МЭК 27000 [1-3]. Стандарты данного семейства являются одними из наиболее динамично развивающихся стандартов в области ИБ.

Проектируемая система в качестве результата своей работы должна предоставлять:

- степень реализации требований семейства стандартов ИСО/МЭК 27000 в легко воспринимаемой форме;
- возможность анализа степени реализации отдельных частей системы управления защитой информации (СУЗИ);
- соотнесение частей СУЗИ конкретным пунктам требований стандартов семейства ИСО/МЭК 27000.

ФУНКЦИОНАЛЬНАЯ ДЕКОМПОЗИЦИЯ СИСТЕМЫ

В силу сложности разрабатываемой системы, была проведена ее предварительная функциональная декомпозиция на отдельные модули для облегчения анализа и дальнейшего проектирования. В результате были выделены:

- центральная управляющая подсистема, задача которой является обобщение предоставленной модулями информации и отображение ее пользователю;
- модули, несущие в себе основную функциональную нагрузку непосредственного контроля реализации требований;
- унифицированный интерфейс взаимодействия управляющей подсистемы с модулями.

ЦЕНТРАЛЬНАЯ УПРАВЛЯЮЩАЯ ПОДСИСТЕМА И ЕЕ МОДУЛИ

Была построена диаграмма вариантов использования верхнего уровня (рис. 1), которая представляет собой множество возможных сценариев взаимодействия пользователей и системы.

Исходя из анализа вариантов использования, была построена диаграмма классов с точки зрения реализации [4] (рис. 2).

В качестве начальных для проектирования модулей были выбраны подмодуль управления целями и средствами контроля и модуль оператив-ного аудита безопасности, так как они характеризуются наименьшим количеством зависимостей от других модулей. Для них также были построены диаграммы вариантов использования и классов.

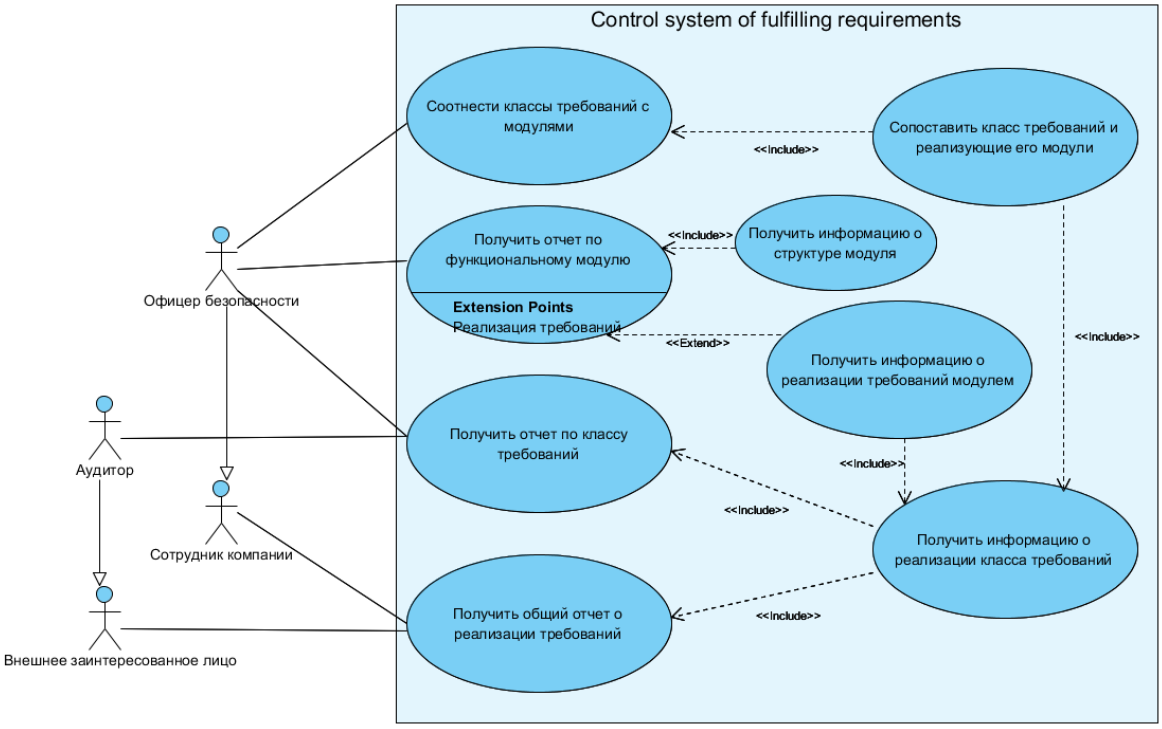

*Рис. 1.*Диаграмма вариантов использования системы контроля реализации требований

ИНТЕРФЕЙС ВЗАИМОДЕЙСТВИЯ

Исходя из требований, предъявляемым к взаимодействию центральной управляющей подсистемы и модулей, были выделены операции, реализуемые данным интерфейсом. Согласно с ними, каждый модуль предоставляет:

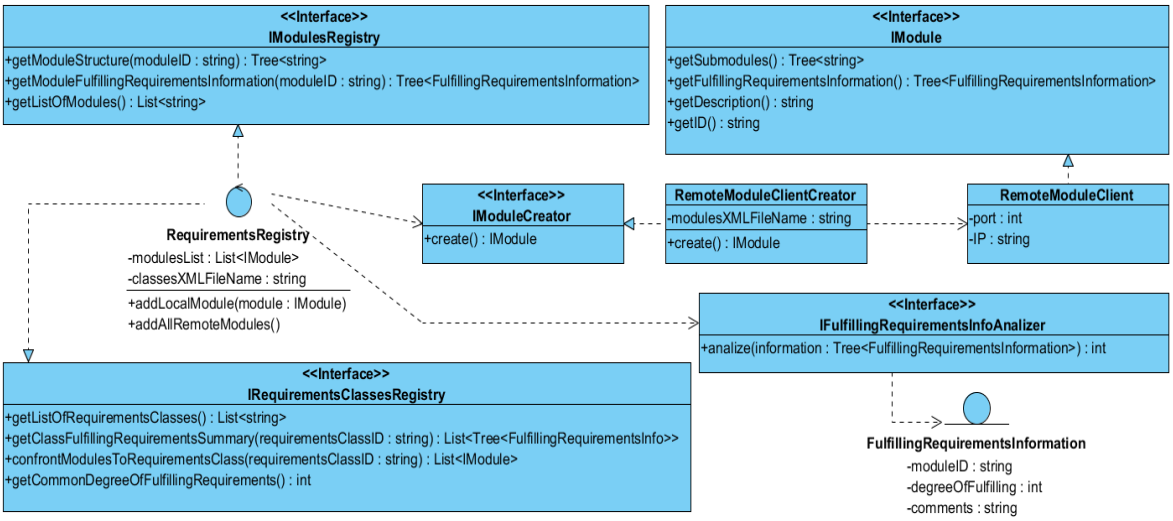

Рис. 2. Диаграмма классов центральной управляющей подсистемы

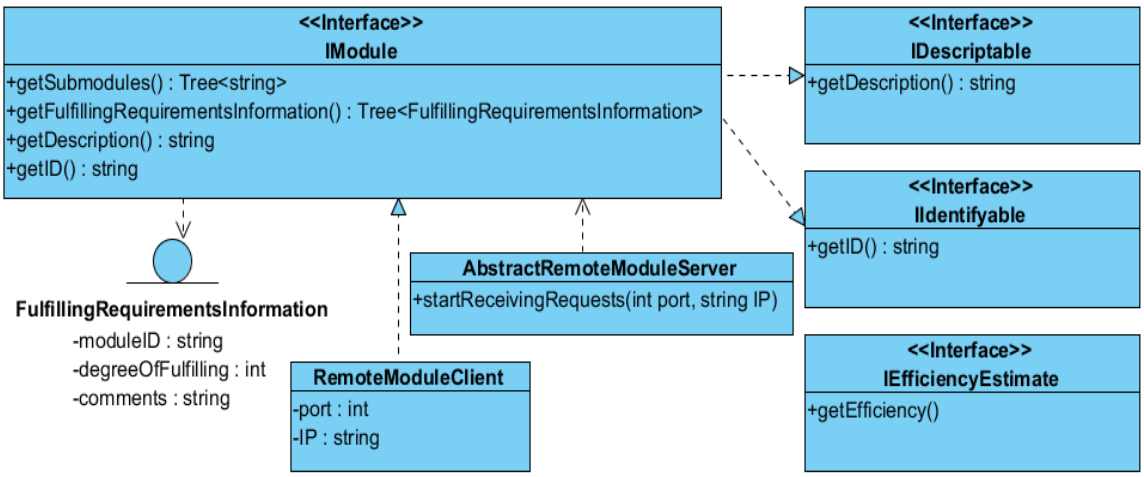

Рис. 3. Интерфейс взаимодействия

- информацию о данном модуле описательного характера;
- информацию о данном модуле идентифицирующего характера;
- дерево подмодулей данного модуля;
- дерево сведений о реализации.

Для формализации степени реализации требований модулем можно было выбрать любой числовой интервал с соответствующей интерпретацией. Однако в данной работе был выбран числовой идентификатор, представляющий собой аналог длины волны света в ангстремах от красного до зеленого, так как он:

- легко сопоставляется близкому человеческому восприятию и интуитивно понятному цветовому спектру;
- позволяет сформулировать процесс реализации требований как переход от красного результирующего цвета к зеленому;
- отражает непрерывность процесса реализации требований.

Таким образом, подсчет результирующей степени реализации сводится к вычислению средней длины волны и определения цвета, ему соответствующего. Данную концепцию также легко можно будет реализовать в виде графического интерфейса.

Данный интерфейс IModule, а также класс информации о текущем модуле FulfillingRequirementsInformation представлены на диаграмме классов (рис. 3). Также здесь представлены классы RemoteModuleClient и AbstractRemoteModuleServer, определяющие механизм сетевого взаимодействия с удаленными модулями.

ЗАКЛЮЧЕНИЕ

На данном этапе была спроектирована модульная система контроля реализации в организации требований стандартов серии ИСО/МЭК

27000, в дальнейшем планируется ее программная реализация в соответствии с унифицированным процессом разработки ПО [5].

Ожидается, что внедрение разрабатываемой системы в организациях, планирующих прохождение процедуры сертификации на соответствие стандартам указанной серии, повысит эффективность этой процедуры, снизит временные и финансовые затраты.

Литература

1. ISO/IEC 27000 «Information technology – Security techniques – Information security management systems – Overview and vocabulary» - первое издание 2009-05-01 - подготовлено Joint Technical Committee ISO/IEC JTC 1.
2. ISO/IEC 27001 «Information technology – Security techniques – Information security management systems – Requirements» - первое издание 2005-10-15 - подготовлено Joint Technical Committee ISO/IEC JTC 1.
3. СТБ П ISO/IEC 27001-2008 «Информационные технологии. Технологии безопасности. Системы управления защитой информации. Требования» - Введ. 2009-03-01. Минск: БелГИСС, 2009.
4. *Фаулер М., Скотт К.* UML основы. М.: Символ-Плюс, 2002.
5. *Якобсон А., Буч Г., Рамбо Дж.* Унифицированный процесс разработки программного обеспечения. СПб.: Питер, 2002.