ФОРМИРОВАНИЕ И ВЕРИФИКАЦИЯ НОРМАТИВНЫХ ПРОФИЛЕЙ КРИТИЧЕСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЗНАНИЕОРИЕНТИРОВАННЫХ МЕТОДОВ

Харченко В.С., Шостак И.В., Манжос Ю.С, Скляр В.В.
Национальный аэрокосмический университет им. Н.Е. Жуковского

Введение. Обоснование необходимости использования средств интеллектуальной поддержки при оценке программного обеспечения.

Эксплуатационные свойства компьютерных систем управления объектами (КСУ) с интенсивным использованием программного обеспечения (аэрокосмическими, энергетическими, транспортными и др.) в большой мере зависит от его качества. В связи с этим при разработке и модернизации таких систем особую важность приобретает организация эффективного оценивания программного обеспечения (ПО). Оценка ПО проводится службами качества, сертификационными центрами, регулирующими органами, в функции которых входит привлечение квалифицированных специалистов достаточно узкого профиля, способных быстро и достоверно оценить свойства ПО в соответствии с классом безопасности. При этом качество оценки практически полностью определяется квалификацией экспертов и имеющимся в их распоряжении информационным ресурсом – базой нормативных документов.

Процедура такой оценки ПО [1] предполагает решение ряда задач, среди которых следует выделить:

- формирование нормативного профиля (НП). НП - это гармонизированные с международными и национальными стандартами совокупности требований, предъявляемых к данному проекту или группе проектов. Нормативными профилями могут быть вновь разрабатываемые государственные или отраслевые стандарты, нормативно-методические документы предприятий и общие требования спецификаций ПО;
- реинжиниринг процесса проектирования ПО и его оценка на основе НП;
- синтаксический и семантический анализ исходного кода ПО с учетом требований НП;

- определение степени соответствия исходного кода ПО проектной документации и НП.

До недавнего времени решение указанных задач, как правило, не вызывало затруднений, поскольку эксперты руководствовались в своих решениях опытом, накопленным на основе большого числа прецедентов, а также интуицией, приобретенной в результате достаточно длительной работы по анализу ПО сравнительно узкого класса систем.

Вместе с тем, устойчивая тенденция к расширению функций, увеличению объема и сложности ПО, а также повышение разнообразия самих объектов, с одной стороны, и необходимость сокращения сроков с одновременным повышением требований к качеству оценки, - с другой, породили ряд проблем в деятельности эксперта.

К этим проблемам относятся:

- большая доля рутинного труда, связанного с анализом существенно расширившейся (за счет международных стандартов) нормативной базы и необходимостью формирования НП ПО уникальных объектов ;
- необходимость синтаксического и семантического анализа значительных объемов ПО (десятков и сотен тысяч операторов);
- возрастание субъективности при оценке соответствия исходного кода ПО проектной документации и НП.

В современных условиях наиболее эффективным средством преодоления указанных проблем является использование в процессе экспертирования ПО методов искусственного интеллекта и инженерии знаний, в частности, экспертных систем.

Применение таких систем обеспечит поддержку эксперта при работе с нормативной базой, а также позволит, путем накопления и обобщения опыта оценок в базе знаний (БЗ) экспертной системы, снизить субъективность принимаемых решений и повысить их эффективность за счет учета большого числа факторов, определяющих свойства анализируемого ПО.

Цель статьи – разработка элементов технологии интеллектуальной поддержки принятия решений экспертом при реализации одной из наиболее важных задач экспертирования ПО – формировании НП.

Характеристика предметной и проблемной областей формирования НП. Профилирование в общем случае включает формирование НП (при разработке ПО или стандартов для него) и верификацию НП (при экспертизе) [2,3].

В ходе формирования НП должен быть проведен синтез (на основе национальной и международной нормативной базы, включающей стандарты ISO, ECSS, IEEE, IAEA и других национальных и международных организаций) профилеобразующей базы (ПОБ) с помощью методов семантического анализа нормативных документов. Из методов семантического анализа в данном случае уместно применить частично–формализованный (вербально-матричный) метод [3], поскольку он максимально приближен к решению задач путем анализа семантических деревьев.

Процесс формирования и верификации НП включает следующие этапы.

1. Отбор и систематизация нормативных документов, формирование на их основе общей профилеобразующей базы (ОПОБ) ПО.

2. Разработка на основе ОПОБ номенклатуры частных профилеобразующих баз (ЧПОБ), исходя из особенностей разработки и применения систем с интенсивным использованием ПО. Формирование множества ЧПОБ.

3. Формирование глоссариев базовых терминов для каждой ЧПОБ.

4. Разработка с помощью глоссариев базовых терминов множества ЧПОБ стандартов-глоссариев для ОПОБ. Формирование профилей терминов.

5. Создание на основе профилей терминов нормативных профилей для каждой ЧПОБ.

Реализация на практике указанных этапов связана с рядом проблем. На первом этапе возникает проблема:

- формирования множества профилеобразующих организаций по критериям, учитывающим их опыт, международный статус, объем и номенклатуру выпущенных стандартов и т. д.;

- ранжирования по этим критериям и их составляющим;

- отбор и систематизацию нормативных документов по каждой из профилеобразующих организаций.

Второй этап порождает проблему определения номенклатуры профилей в соответствии с различными аспектами создания и функционирования ПО (проектные требования, жизненный цикл, инструментальные средства разработки, методы оценки и др.)

Третий и четвертый этапы связаны с необходимостью семантического анализа и сопоставления терминов в нормативных документах различных стандартов, а также синтеза глоссариев терминов, однозначно толкуемых во всех используемых при экспертировании ПО системах стандартов.

Реализация пятого этапа предполагает учет (при формировании НП на основе ЧПОБ) большого числа факторов, определяемых особенностями разработки и применения конкретного ПО.

Перечисленные выше проблемы относятся к разряду трудно формализуемых, комплексное их решение затруднено из-за отсутствия эффективных аналитических методов. Исходя из этого целесообразно в процессе формирования и верификации НП использовать интеллектуальные методы.

Вместе с тем, ряд частных задач при формировании и верификации НП может быть успешно решен с использованием аналитических методов и традиционной обработки данных. К этим задачам относятся, в первую очередь, выбор наиболее представительных нормативных документов, формирование таблиц требований из одной группы для этих документов и т. д.

Кроме того, можно выделить еще ряд задач, связанных с разработкой:

- стратегии тестирования, набора тестовых заданий для апробирования методов и алгоритмов частично- формализованного и семантического анализа. Для тестирования используются нормативные документы, разработанные в Украине и международными организациями ISO, IEC, IAEA и др., для задания требований к ПО систем , важных для безопасности АЭС;
- информационно- аналитических утилит поддержки процесса частично-формализованного анализа (ЧФА) ПОБ;
- интеллектуальных утилит поддержки знаниеориентированного семантического анализа (ЗСА) текстовых документов из ПОБ (синтеза

локальных и глобальных семантических деревьев) и сравнения результатов профилирования различными (ЧФА и ЗСА) методами.

Таким образом, компьютерная поддержка процесса формирования и верификации НП может быть организована на основе интегрированной системы, сочетающей в себе традиционные методы и средства обработки данных с возможностями знаниеориентированных методов.

Концепция построения интеллектуальной интегрированной системы формирования и верификации НП. Рассмотрим особенности построения интеллектуальной интегрированной системы формирования и верификации НП (ИСФВП) в четырех основных аспектах, характерных для любой системы искусственного интеллекта: выявления знаний, представления знаний, манипулирования знаниями, способа реализации вывода на знаниях.

Процесс выявления знаний в данном случае основан преимущественно на текстологических источниках (нормативной базе) и может быть реализован традиционными методами семантического анализа.

Знания в ИСФВП наиболее удобно представлять в виде фреймов [4], поскольку ПОБ имеет четко выраженную иерархическую структуру. Структуры элементов одного и того же уровня стереотипны. Механизм активизации фреймов различных уровней и присоединенные процедуры отдельных слотов в этом случае представляются в форме метаправил и обычных правил продукций соответственно.

Проиллюстрируем описанный выше вариант организации базы знаний (БЗ) ИСФВП на примере структуры стандартов Европейского космического агентства (ESA) [5]. Рассматриваемая система стандартов имеет семиуровневую фреймовую структуру:

1. фрейм верхнего уровня -ESA;
2. уровень групп стандартов (например, ESA PSS);
3. уровень экземпляров стандартов (ESA PSS 05.0);
4. уровень руководств (ESA PSS 05.04);
5. уровень разделов руководств (ESA PSS 05.02 2);
6. уровень пунктов разделов (ESA PSS 05.04 2.3);
7. уровень подпунктов (ESA PSS 05.04 2.3.3).

Активизация фреймов трех верхних уровней осуществляется метаправилами типа:

ЕСЛИ Космический аппарат ТО ESA;

ЕСЛИ ESA И Проектирование ПО ТО ESA PSS;

ЕСЛИ ESA PSS И Архитектурное проектирование ТО ESA PSS 05.4.

Внутри отдельного экземпляра стандарта (начиная с четвертого уровня и ниже) метаправила активизации фреймов строятся в соответствии с оглавлением, например:

ЕСЛИ ESA PSS 05.0 И Средства разработки архитектурного проекта ТО Гл.4(Стр. 35);

ЕСЛИ ESA PSS 05.0 И Гл.4(Стр. 35) ТО 4.1 Введение (Стр.35) И 4.2 Средства разработки для построения физической модели (Стр. 35) И Средства разработки для спецификации проекта (Стр.35);

ЕСЛИ ESA PSS 05.0 И 5.2 Стиль (Стр. 37) ТО 5.2.1 Ясность (Стр.37) И 5.2.2 Корректность (Стр. 37) И 5.2.3 Модифицируемость (Стр. 38).

Требования к ИСФВП. Исходя из приведенного выше анализа предметной и проблемной областей процесса формирования НП при экспертировании ПО, может быть сформулирован ряд системотехнических требований к построению ИСФВП:

1. Тип системы - интеллектуальная интегрированная система поддержки принятия решений (ИИСППР);

2. Форма представления знаний в БЗ ИСФВП – фреймово-продукционная, с использованием метаправил;

3. Источники знаний ИСФВП – преимущественно текстологические;

4. Выявление знаний – автоматизированный анализ текстов, анкетирование экспертов;

5. Активизация процесса вывода на знаниях (ВНЗ) – по запросу пользователя;

6. Стратегии и схемы ВНЗ: прямой вывод по схеме «вширь», обратный вывод.

Выводы. Качество формирования и верификации НП для критического ПО существенно влияет на уровень безопасности КСУ.

Задача формирования и верификации НП является одной из основных задач процесса разработки и экспертизы критического ПО.

Учитывая постоянно расширяющуюся нормативную базу в области ПО, решение задач формирования НП (включая и разработку самих стандартов) целесообразно формализовать в направлении повышения верифицируемых требований, содержащихся в них.

В основу разработки интеллектуальной интегрированной системы формирования и верификации НП следует положить процедуры частично формализованного анализа текстов (требований стандартов) и процедуры построения и объединения семантических деревьев, полученных при анализе документов ПОБ.

При разработке ИИС реализуются принципы:

- диверсности или проектного многообразия, характерного для технологий создания критического ПО [6]. Использование двух альтернативных методов анализа (ЧФА и ЗСА) обеспечивает повышение достоверности решения задачи;

- разработки системы с использованием технологии группового взаимодействия (BPwin, Rational Rose, MS Project и др.), обеспечивающих постановку задач, планирование, синхронизацию и контроль выполнения проекта;

- ориентации на оболочку экспертной системы JESS, других апробированных программных продуктов. Их выбор определяется, исходя из критерия «надежность-стоимость».

Список источников

1. Vilkomir S.A., Kharchenko V.S. An «Asymmetric» Approach to the Assessment of Safety-Critical Software During Sertification and Licensing //Proceedings of ESCOM-SCOPE 2000 Conference, 18-20 April, 2000, Munich, Germany.- Pp 467-475.

2. Харченко В.С., Ястребенецкий М.А., Васильченко В.Н. Нормирование и оценка безопасности информационных и управляющих АЭС: регулирующие требования к программному обеспечению // Ядерная и радиационная безопасность,- 2002.- №1.- С.18-33.

3. Kharchenko V.S., Vilkomir S.A. The Formalized Models of an Evaluation of a Verification Process Of Critical Software // Proceedings PSAM5, November 27-December 1, 2000, Osaka, Japan.- Vol. 4.- Pp 2383-2388.

4. Шостак И.В. Текущее состояние базы знаний в динамических экспертных системах управления сложными объектами // Радиоэлектроника и информатика.- 2000.- №3.- С.68-71.

5. Конорев Б.М. и др. Нормативная база программной инженерии в разработке систем с интенсивным использованием программного обеспечения.- Харьков: Национальный аэрокосмический университет им. Н.Е.Жуковского "ХАИ".-2001.- 162С.