УДК 004.052.42

Сертификация и верификация программных средств

А.А. Агапов,
канд. техн. наук, директор по информационным технологиям

ЗАО НТЦ ПБ

Е.А. Агапова,
мл. науч. сотрудник

АНО «Агентство исследований промышленных рисков»

Приводится сравнение процедур сертификации программных средств, применяемой для подтверждения соответствия их нормативным и методическим документам в России, и верификации (валидации), используемой за рубежом.

Comparison of the software certification procedures applied for confirmation of their compliance with the normative and methodical documents in Russia, and verification (validation) of the software used abroad is given in the Article.

Ключевые слова: сертификация программных средств, тестирование, верификация, валидация, Протокол оценки модели, TOXI+Risk, FLACS.

Один из критериев, подтверждающих качество программного продукта, — наличие сертификата соответствия, который выдает аккредитованный в системе сертификации ГОСТ Р орган по сертификации программной продукции в определенной области.

Законодательством предусмотрена главным образом добровольная сертификация[1] программных средств (за исключением отдельных, специально оговоренных, случаев, например программных средств в области связи, которые попадают в Перечень средств связи, подлежащих обязательной сертификации, утвержденный постановлением Правительства Российской Федерации от 25 июня 2009 г. № 532, или в области защиты информации в соответствии с Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781).

Для некоторых групп программных средств, например связанных с расчетами пожарного риска, обязательность сертификации законодательно не установлена и требование применения при выполнении расчетов только сертифицированного программного обеспечения устанавливают ведомственными административными и распорядительными документами. Фактически это равносильно требованию обязательной сертификации расчетных программ.

Сертификацию проводят для подтверждения соответствия программного продукта конкретным методическим документам, а также требованиям государственных стандартов в области информационных технологий (в части программного интерфейса, документации и т.д.). Процедуру проверки соответствия выполняют в аккредитованной испытательной лаборатории по специальной методике испытаний. В общем случае методика испытаний предполагает, что при вводе некоторого набора исходных данных на выходе расчетного модуля должен получаться ожидаемый результат, который соответствует определенным формулам, указанным в нормативном (методическом) документе, на соответствие которому выполняется сертификация. Если рассчитанная величина совпадает с ожидаемой, испытательная лаборатория дает заключение о соответствии, на основании чего орган по сертификации выдает сертификат установленной формы. Список нормативных документов, для которых подтверждено соответствие проверяемого программного средства, приводится в сертификате и приложении к нему. В качестве примера на рисунке представлен сертификат соответствия на программный продукт TOXI+Risk [1, 2].


СЕРТИФИКАТ СООТВЕТСТВИЯ

▲ **Сертификат соответствия TOXI+Risk в системе сертификации ГОСТ Р**

Отметим, что для расчета пожарного риска точное соответствие результатов расчета методикам, утвержденным соответствующими приказами МЧС России [3, 4], — обязательное условие. При этом заложен-

[1] Сертификация (лат. sertifico — удостоверяю) — подтверждение соответствия качественных характеристик товара стандартам качества. Под сертификацией подразумевается также процедура получения сертификата. URL: http://ru.wikipedia.org.

ный в методике консерватизм расчетных алгоритмов (выбор худших, опасных с точки зрения получаемого результата допущений) вполне логичен, принимая во внимание тот факт, что полученные результаты расчета используют для принятия управленческих решений по вопросам пожарной безопасности.

Похожий подход до недавнего времени использовали и применительно к вопросам промышленной безопасности. В то же время упомянутый консервативный подход к моделированию последствий возможных аварий в достаточно большом числе случаев не является оправданным, поскольку, во-первых, вероятность возникновения консервативных условий подчас чрезвычайно мала, а во-вторых, простые параметрические методы расчета не позволяют учесть специфику конкретной задачи. В том числе поэтому в п. 10.5 Федеральных норм и правил в области промышленной безопасности «Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств» наряду с официально утвержденными расчетными методиками предусмотрено обоснованное использование иных методов расчета [5].

Таким образом, наряду с проведением расчетов по формулам, приведенным в нормативном документе, расчетчику предоставляется возможность более гибкого использования расчетных инструментов. Безусловно, последние должны выдавать заслуживающие доверия (в первую очередь для контролирующих органов) результаты, которые подтверждаются экспериментальными данными или фактическими последствиями (фактическими данными) аварий. При этом используемые в компьютерных программах математические модели могут включать сложные системы дифференциальных уравнений, правильность решения которых, как правило, невозможно проверить простыми расчетами на калькуляторе. Поэтому упомянутая выше стандартная процедура тестирования на проверку соответствия в этом случае уже неприменима. Критерий правильности работы программы — соответствие полученных результатов фактическим данным. Часто эту процедуру называют верификацией[1] программного обеспечения.

Нужно отметить, что в контексте проверки программного обеспечения в литературе встречаются и другие термины, например «валидация»[2]. Термины «тестирование»[3], «верификация» и «валидация» программного обеспечения в общем случае обозначают разные уровни проверки корректности работы программной системы, однако для однозначности далее будем использовать термин «верификация».

Одним из наиболее сложных моделируемых явлений признано рассеяние опасных веществ (в том числе взрывопожароопасных) в атмосфере. В то же время от корректности результатов моделирования рассеяния аварийных выбросов зависит корректность оценок дальнейших последствий аварии: взрыва топливно-воздушной смеси, пожара-вспышки, токсического воздействия и др. Причем, если простейшие консервативные модели рассеяния (так называемые гауссовы модели) выражаются несложными параметрическими функциями, то более сложные модели (например, модели тяжелого газа; модели, учитывающие геометрию окружающего пространства в месте выброса) задаются сложными системами дифференциальных уравнений, в которых используют различные эмпирические коэффициенты. Верификация этих моделей, как правило, совмещена с верификацией соответствующих компьютерных программ, в которых эти модели реализованы. Так, верификацию методики рассеяния по модели тяжелого газа, которая в дальнейшем получила статус руководящего документа Ростехнадзора — РД-03-26—2007 [6], проводили с использованием программного комплекса TOXI+ путем сопоставления полученных результатов с данными натурных экспериментов [7–10]. Верификацию иностранных программных средств, связанных с моделированием рассеяния (PHAST, FLACS и др.), проводят аналогичным образом.

Для иностранных разработок, как и для отечественных, остаются открытыми вопросы достаточности верификационных испытаний, их адекватности и официального подтверждения соответствия результатов фактическим данным. Причем для отечественных разработок, реализующих модели, которые входят в нормативные методические документы, таким официальным подтверждением становится сертификат соответствия, а для иностранных программных разработок, некоторые из которых используют во всем мире, — научные публикации и репутация разработчика. В то же время формализованные критерии оценки корректности использованной в программе математической модели до недавнего времени отсутствовали.

В целях формализации процедуры верификации различных моделей рассеяния при авариях с выбросом сжиженного природного газа (СПГ) в 2007 г. Национальной ассоциацией противопожарной защиты (NFPA, США) разработан Протокол оценки модели. При верификации предполагается провести расчеты по исходным данным 33 специально подобранных натурных экспериментов с выбросом СПГ и фреона для различных условий и сравнить полученные результаты расчета с показаниями датчиков.

---

[1] Верификация — подтверждение посредством представления объективных свидетельств того, что установленные требования были выполнены (ИСО 9000).

[2] Валидация — подтверждение посредством представления объективных свидетельств того, что требования, предназначенные для конкретного использования или применения, выполнены (ИСО 9000).

[3] Тестирование программного обеспечения — процесс исследования, испытания программного продукта, имеющий две различные цели: продемонстрировать разработчикам и заказчикам, что программа соответствует требованиям; выявить ситуации, в которых поведение программы является неправильным, нежелательным или не соответствующим спецификации (URL: http://ru.wikipedia.org).

Для подтверждения корректности математической модели и соответствующего программного продукта требуется, чтобы статистические отклонения между результатами расчетов и замеров лежали в заданном допустимом диапазоне.

На с. 60 журнала приведен сокращенный перевод статьи «Валидация программного комплекса FLACS в части рассеяния газа при разливе сжиженного природного газа: Протокол оценки модели» [11], в которой изложены результаты тестирования известного программного продукта FLACS для трехмерного моделирования аварий с выбросом опасных веществ разработки фирмы GexCon (Норвергия). Описанные в статье исходные данные для проведения расчетов и полученные результаты без сомнения могут представлять интерес как для разработчиков моделирующих программ, так и для расчетчиков.

Список литературы

1. *Использование* программного комплекса «ТОХІ+^{Risk}» для оценки пожарного риска/ А.А. Агапов, И.О. Лазукина, А.Л. Марухленко и др.// Безопасность труда в промышленности. — 2010. — № 1. — С. 46–52.

2. *Программно-аппаратный* комплекс «ТОКСИ+Метео» для оценки последствий возможных аварий с учетом данных о текущих погодных условиях/ А.А. Агапов, И.О. Хлобыстова, А.Л. Марухленко и др.// Безопасность труда в промышленности. — 2011. — № 1. — С. 22–25.

3. *Методика* определения расчетных величин пожарного риска на производственных объектах: утв. приказом МЧС России от 10 июля 2009 г. № 404// Декларирование пожарной безопасности и оценка риска: сб. док. — Сер. 19. — Вып. 2. — М.: ЗАО НТЦ ПБ, 2014. — С. 100–181.

4. *Методика* определения расчетных величин пожарного риска в зданиях, сооружениях и строениях различных классов функциональной пожарной опасности: утв. приказом МЧС России от 30 июня 2009 г. № 382// Декларирование пожарной безопасности и оценка риска: сб. док. — Сер. 19. — Вып. 2. — М.: ЗАО НТЦ ПБ, 2014. — С. 31–99.

5. *Общие* правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств: федер. нормы и правила в обл. пром. безопасности. — Сер. 09. — Вып. 37. — М.: ЗАО НТЦ ПБ, 2015. — 126 с.

6. *РД-03-26—2007.* Методические указания по оценке последствий аварийных выбросов опасных веществ. — Сер. 27. — Вып. 6. — М.: ЗАО НТЦ ПБ, 2008. — 124 с.

7. *Методика* расчета распространения аварийных выбросов, основанная на модели рассеяния тяжелого газа/ А.А. Шаталов, М.В. Лисанов, А.С. Печеркин и др.// Безопасность труда в промышленности. — 2004. — № 9. — С. 46–52.

8. *Верификация* методик оценки последствий аварийных выбросов газа от источников продолжительного действия/ М.В. Лисанов, А.С. Печеркин, А.В. Пчельников и др.// Безопасность труда в промышленности. — 2005. — № 8. — С. 28–35.

9. *Сравнение* результатов моделирования аварийных выбросов опасных веществ с фактами аварий/ С.И. Сумской, К.В. Ефремов, М.В. Лисанов и др.// Безопасность труда в промышленности. — 2008. — № 10. — С. 42–50.

10. *Сравнение* результатов расчетов последствий аварийных выбросов опасных веществ по программным комплексам ТОКСИ+ и PHAST / М.В. Лисанов, К.В. Ефремов, С.И. Сумской и др.// Безопасность труда в промышленности. — 2011. — № 2. — С. 56–60.

11. *Olav R. Hansen, Mathieu Ichard, Scott G. Davis.* Validation of FLACS for Vapor Dispersion from LNG Spills: Model Evaluation Protocol// 12-th Annual International Symposium of the Mary Kay O'Connor Process Safety Center, 27–28 Oct. 2009, Texas A&M University, College Station.

inform@safety.ru

Материал поступил в редакцию 11 марта 2015 г.

Валидация программного комплекса FLACS в части рассеяния газа при разливе сжиженного природного газа: Протокол оценки модели[1]

Олав Р. Хансен, Мэтью Ичард, Скотт Г. Дэвис

Для оценки последствий разливов сжиженного природного газа (СПГ) и его рассеяния в атмосфере существует большое количество различных математических моделей. Анализ опасностей, связанных с крупными выбросами СПГ, обычно проводят в три этапа: определяют характеристики выброса СПГ, моделируют рассеяние образовавшегося облака опасного газа (топливно-воздушной смеси — ТВС) в атмосфере и оценивают барическое и тепловое воздействие при воспламенении облака ТВС или пожаре пролива.

Как правило, анализ этих этапов выполняют отдельно и, например, результаты расчетов по первому этапу используют как исходные данные для второго.

[1] Адаптированный сокращенный перевод А.А. Агапова и Н.М. Случек (ЗАО НТЦ ПБ) статьи Olav R. Hansen, Mathieu Ichard and Scott G. Davis «Validation of FLACS for Vapor Dispersion from LNG Spills: Model Evaluation Protocol».