РАЗВИТИЕ СТАНДАРТИЗАЦИИ В ОБЛАСТИ НАДЁЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В.Л. Николаенко, П.С. Почиковский, Г.В. Сечко, Т.Г. Таболич

Белорусский Государственный Университет Информатики и Радиоэлектроники,
кафедра защиты информации,
П. Бровки 6, г. Минск, Беларусь,
телефон: (+37517)2932317, e-mail: tabolichtatiana@mail.ru

В докладе обсуждаются достоинства и недостатки ГОСТа 27.205–97. «Надёжность в технике. Проектная оценка надёжности сложных систем с учётом технического и программного обеспечения и оперативного персонала», хотя это следовало делать до его внедрения Необходимость такого обсуждения вызвана тем, что разработчики стандарта хотя и спорным способом, но впервые попытались оценить совокупную надёжность технического и программного обеспечения оборудования.

Ключевые слова: надежность, оперативный персонал, оценка, программное обеспечение, стандартизация, техническое обеспечение.

1 ВВЕДЕНИЕ

Получив от СССР стройную систему стандартов «Система стандартов «Надёжность в технике», независимые государства СНГ попытались её усовершенствовать. Для координации работ по надёжности между странами СНГ был создан международный технический комитет (МТК) 119 «Надёжность в технике», куда вошли почти все страны СНГ. В рамках этого комитета украинской ассоциацией «Надёжность машин и сооружений» в 1997 году был разработан проект стандарта [1]. Вслед за разработкой последовало внедрение одноимённых ГОСТов в Украине, Средней Азии и Закавказье. Россия от внедрения стандарта отказалась. Стандарт просуществовал внедрённым в перечисленных странах 8 лет, после чего в 2005 году были принят в РБ в качестве государственного.

2 ОСНОВНАЯ ЧАСТЬ

Однако внимательное изучение ГОСТа [1] в БГУИР показало наличие в нём математических ошибок. По письму БГУИР в БелГИСС последний подготовил изменение [2], введённое в действие с 01.11.2008 Постановлением Госстандарта Республики Беларусь № 16 от 31.03.2008 и исправившее имевшиеся в [1] ошибки и ряд других недостатков. При этом проект изменения [2] за год до своего внедрения был разослан на отзыв организациям и учреждениям республики, в которых занимаются надёжностью. Все отзывы, кроме отзыва БГУИР, поступили без замечаний. Видимо, поэтому в [1] остались спорные моменты. Дело в том, что в ГОСТе [1] признаётся только один из возможных вариантов оценки надёжности программного обеспечения, не оставляя другим вариантам права на существование. Принятый вариант не свободен от замечаний.

Например, классификация отказов ПО на обнаруженную ошибку (защитный отказ ПО), необнаруженную ошибку (скрытую ошибку) и зацикливание вследствие дефекта ПО не очевидна, тем более что до принятия изменения [2] эта же классификация выглядела следующим образом: обнаруживаемая неверная обработка входного набора данных (защитный отказ ПО), необнаруживаемая неверная обработка входного набора данных (скрытая ошибка) и зацикливание вследствие дефекта ПО. Сравнение вышеприведенных классификаций показывает, что они не идентичны друг другу.

В [1] предложен показатель безошибочности ПО в отношении некоторой функции функциональной подсистемы программного обеспечения (понятие функциональной подсистемы, скомпонованной для выполнения отдельной функции, вводится стандартом). Данный показатель по мнению авторов стандарта позволяет рассчитать среднюю наработку на проявление дефектов ПО и вероятность того, что имеющиеся дефекты ПО не проявятся в течение заданного времени. Действительно, показатель безошибочности согласно стандарта является входным аргументом вышеуказанных наработки и вероятности. Однако в том же стандарте указано, что: «...Показатель безошибочности позволяет рассчитать среднюю наработку ... и вероятность... при наличии ряда необходимых дополнительных данных». Откуда взять эти дополнительные данные, стандарт умалчивает.

Проблематично также рассчитать предложенные в стандарте характеристики надёжности оперативного персонала. Стандарт для такого расчёта регламентирует показатели, сходные с аналогичными характеристиками программного обеспечения, – показатель безошибочности оперативного персонала, среднюю наработку функциональной подсистемы оперативного персонала на ошибку и вероятность отсутствия ошибки оперативного персонала в течение заданного времени. Эти показатели, как и в предыдущем абзаце для программного обеспече-

ния, без дополнительных данных рассчитать также практически невозможно.

Возможность применения на практике предложенной в стандарте методики оценки надёжности отдельно по функциональным подсистемам и сведения затем рассчитанных показателей в общие показатели надёжности всей системы, состоящей из указанных функциональных подсистем, не подтверждена формулами или примером. Если все подсистемы считать независимыми друг от друга (применять последовательное соединение подсистем в надёжностном смысле), то неясно, как оценить надёжность двухфункциональной системы, технические средства для отдельных функций которой являются различными, а программное обеспечение одно и то же. Действительно, одна и та же программа не может быть независимой сама от себя. Видимо, поэтому иллюстрирующий методику пример выполнен для однофункциональной системы.

Приведенные в стандарте примеры расчёта в свою очередь также не являются убедительными и корректными. Например, в качестве исходных данных для расчёта надёжности комплекса технических средств относительно однократных ошибок в двоичном слове приняты средняя наработка на отказ, равная 12 часам, и среднее время восстановления работоспособного состояния оборудования, равное 12 мин. Возникает справедливый вопрос: что это за качество ремонта и восстановления оборудования для обработки двоичных слов, при котором на восстановление тратится очень мало времени (12 мин), зато через 12 часов после такого восстановления оборудование снова отказывает? Может, более целесообразно в течение дня разобраться в причинах появления однократных ошибок в двоичном слове, разработать соответствующие мероприятия по повышению надёжности, внедрить их, а затем не иметь отказов по этой причине в течение нескольких лет.

Необходимо отметить также не совсем удачное изменение пункта А.4 стандарта, проведенное в [2]. Изменение [2] исключает четвёртый абзац, в котором речь шла об устранении отказов-аварий системы за счёт корректировки их другими видами обеспечений. Однако третий абзац пункта А.4, звучавший ранее как «повышается также средняя наработка на отказ вида «Остановка»...», изменением [2] скорректирован к виду: «За счёт того, что полностью устраняются отказы-аварии системы, несколько понижается средняя наработка на отказ вида «Остановка»...». Вывод нелогичный – отказы устранены, безотказность должна повыситься, а она понизилась. В варианте до изменения безотказность повышалась, но только за счёт неверного математического расчёта.

Кроме того, если свойство устойчивости ПО к некоторым отказам КТС повышает безотказность отказов типа «скрытое неверное функционирование» (второй абзац пункта А.4), то непонятно, почему это же свойство должно снижать безотказность системы относительно отказов вида «Остановка», о чём говорилось выше.

Следует отметить также, что одновременно со стандартом [1] был внедрён стандарт [3], также содержащий грубейшую ошибку (формула экспоненциального распределения, на наш взгляд, одного из наиболее употребительных распределений в области надёжности). Хорошо, что ошибка исправлена изменением [4].

3 ЗАКЛЮЧЕНИЕ

В докладе обсуждаются достоинства и недостатки стандарта [1], хотя это следовало делать до его внедрения. Необходимость такого обсуждения вызвана тем, что разработчики стандарта хотя и спорным способом, но всё же впервые попытались оценить совокупную надёжность технического и программного обеспечения оборудования (как дополнительно учесть надёжность оперативного персонала, в стандарте не показано). В этих условиях цель доклада – на примере стандарта [1] ещё раз подчеркнуть важность стандартизации в области надёжности программного обеспечения.

ЛИТЕРАТУРА

[1] ГОСТ 27.205–97. Надёжность в технике. Проектная оценка надёжности сложных систем с учётом технического и программного обеспечения и оперативного персонала. Основные положения. – Мн.: Госстандарт РБ, 2005.

[2] Изменение № 1 BY* ГОСТ 27.205–97. Надёжность в технике. Проектная оценка надёжности сложных систем с учётом технического и программного обеспечения и оперативного персонала. Основные положения. – Мн.: Госстандарт, 2008.

[3] ГОСТ 27.005–97. Надёжность в технике. Модели отказов. Основные положения. – Мн.: Госстандарт РБ, 2005.

[4] Изменение № 1 BY* ГОСТ 27.005–97. Надёжность в технике. Модели отказов. Основные положения. – Мн.: Госстандарт, 2008.