УДК - 004.4.056 + 004.4.052 Вестник УрФО № 1(23) / 2017, с. 20–23

Юганссон А.Н., Заколдаев Д.А.

РАЗРАБОТКА МЕТОДИКИ ДЛЯ РАСЧЕТА ОЦЕНКИ ТЕХНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ СРЕДСТВ

На сегодняшний день, программное обеспечение занимает ключевую роль во всех информационных процессах общества. Зачастую, вопросы надежности программного обеспечения задвигаются на второй план при проектировании и разработке программных средств в угоду скорейшего вывода программного продукта на рынок. В данной статье предлагается решение, позволяющие оценить технологическую безопасность разработанного продукта для дальнейшей минимизации рисков, связанных с его эксплуатацией и технической поддержкой.

Ключевые слова: *технологическая безопасность программных средств, надежность программного обеспечения, методика расчета оценки.*

Iuganson A., Zakoldaev D.

A CALCULATION METHODOLOGY OF ASSESS FOR SOFTWARE TECURITY

Nowadays software plays a key role in different information processes. However, software reliability becomes underestimated during its construction and developing. The deployment of new product may lead to various loss due to lack in software architecture and programming defects. In this article a new methodology was developed for calculation of assess for software tecurity. This metric may help to minimize economic risks on stages of exploitation and technical maintenance.

Keywords: *software reliability, software tecurity, calculation methodology.*

Вопросы технологической безопасности программных средств (ПС) с каждым днем становятся все более актуальными. По результатам аналитического исследования, проведенного компанией НПО «Эшелон» в 2012 году[1], были сделаны выводы: ситуация в области защищенности приложений не улучшается с течением времени. Менеджмент процесса разработки находится на низком уровне, что в свою очередь ведет к увеличению числа ошибок в программном коде и, как следствие, увеличению затрат на выпуск конечного продукта. По данным исследования, выполненного по заказу Национального института стандартов и технологий США, убытки, возникающие из-за слабого развития инфраструктуры устранения дефектов в ПО (уязвимостей и ошибок программирования), достигают 60 миллиардов долларов в год[2]. Стоимость устранения дефекта, пропущенного на этапах разработки и тестирования, может возрасти после поставки программы многократно[3].

ний день типовая методика для расчета оценки технологической безопасности ПС попросту отсутствует. Существующие работы (см. 5, 6) не могут обеспечить в должной мере повторяемость и воспроизводимость результатов испытания.

Таким образом, задача разработки и совершенствования методического обеспечения расчета оценки технологической безопасности ПС в настоящее время является актуальной.

Типовая методика расчета оценки (рис. 1) представляет собой вычисление определенного набора метрик, полученных при проведении испытаний. Для формирования множества типовых метрик была использована методика, предлагаемая стандартом ГОСТ 28195-89, оптимизированная с учетом особенностей исследуемых программных средств.

На первом этапе происходит вычисление расчетных элементов метрик:

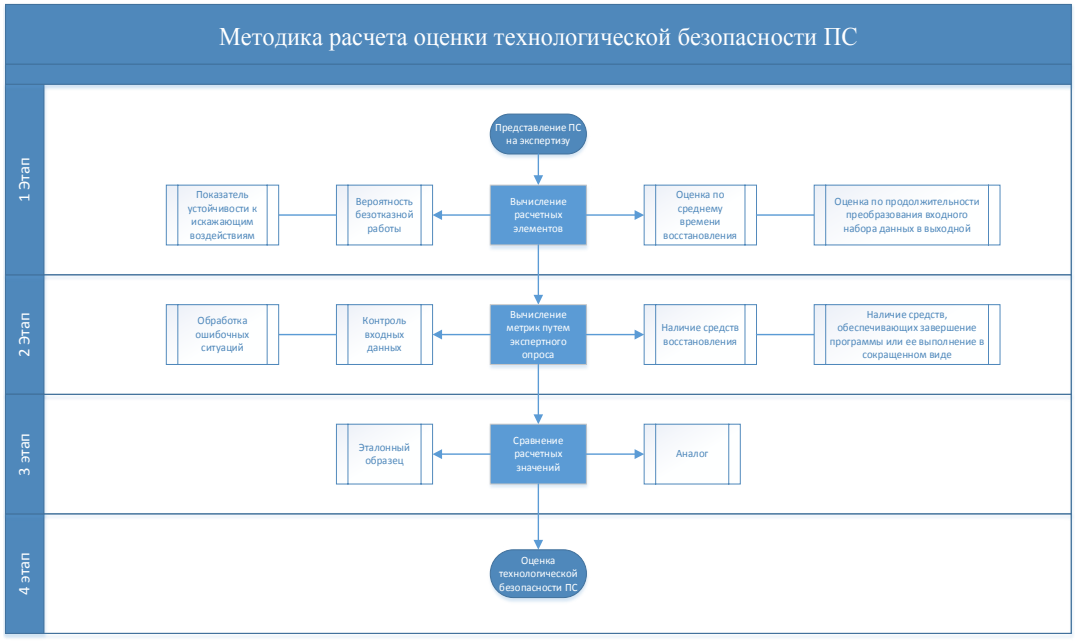

Рис. 1. Методика расчета оценки технологической безопасности ПС

Под технологической безопасностью ПС понимается совокупность свойств, характеризующих способность программы сохранять заданный уровень пригодности в заданных условиях в течение заданного интервала времени, где в качестве ограничения уровня пригодности рассматриваются дефекты безопасности и уязвимости[4].

Необходимо признать, что на сегодняш-

– показатель устойчивости к искажающим воздействиям, вычисляемый по форму-

$$P = 1 - \frac{D}{K} \qquad (1),$$

ле:

где D – число экспериментов, в которых искажающие воздействия приводили к отказу;

K – число экспериментов, в которых имитировались искажающие воздействия.

– вероятность безотказной работы, вычисляемая по формуле:

$$P = 1 - \frac{Q}{N} \quad (2),$$

где Q – число зарегистрированных отказов;

N – число экспериментов.

– оценка по среднему времени восстановления, вычисляемая по формуле:

$$Q_{â} = \begin{cases} 1, \text{åñëè } \text{Ò}_{â} \le \text{Ò}_{â}^{äîï} \\ T_{â}^{äîï} \Big/ T_{â}, \text{åñëè } \text{Ò}_{â} > \text{Ò}_{â}^{äîï} \end{cases} \quad (3),$$

где $\text{Ò}_{â}^{äîï}$ – допустимое среднее время восстановления;

$$\dot{O}_{â} = \frac{1}{N} \sum_{i}^{N} T_{âi} \quad (4),$$

$\text{Ò}_{â}$ – среднее время восстановления, которое определяется по формуле:

где N – число восстановлений;

$T_{âi}$ –время восстановления после i-го отказа.

– оценка по продолжительности преобразования входного набора данных в выходной, вычисляемая по формуле:

$$Q_{â} = \begin{cases} 1, \text{åñëè } \text{Ò}_{ïi} \le \text{Ò}_{ïi}^{äîï} \\ T_{ïi}^{äîï} \Big/ T_{ïi}, \text{åñëè } \text{Ò}_{ïi} > \text{Ò}_{ïi}^{äîï} \end{cases} \quad (5),$$

где $\text{Ò}_{ïi}^{äîï}$ – допустимое время преобразования i-го входного набора данных;

$\text{Ò}_{ïi}$ – фактическая продолжительность преобразования i-го входного набора данных.

На втором этапе дается оценка метрикам, вычисляемым методом экспертного опроса (0 – ПС не удовлетворяет требованиям метрики, 1 – удовлетворяет):

– наличие требований к программе по устойчивости функционирования при наличии ошибок во входных данных;

– возможность обработки ошибочных ситуаций;

– полнота обработки ошибочных ситуаций;

– наличие тестов для проверки допустимых значений входных данных;

– наличие системы контроля полноты входных данных;

– наличие средств контроля корректности входных данных;

– наличие средств контроля непротиворечивости входных данных;

– наличие требований к программе по восстановлению процесса выполнения в случае сбоя операционной системы, процессора, внешних устройств;

– наличие требований к программе по восстановлению результатов при отказах процессора, ОС;

– наличие средств восстановления процесса в случае сбоя оборудования;

– наличие возможности разделения по времени выполнения отдельных функций программ;

– наличие возможности повторного старта с точки останова;

– наличие проверки параметров и адресов по диапазону их значений;

– наличий обработки граничных результатов;

– наличие обработки неопределенностей;

– наличие централизованного управления процессами, конкурирующими из-за ресурсов;

– наличие возможности автоматически обходить ошибочные ситуации в процессе вычисления;

– наличие средств, обеспечивающих завершение процесса решения в случае помех;

– наличие средств, обеспечивающих выполнение программы в сокращенном объеме в случае ошибок и помех.

На третьем этапе расчетные значения сравниваются с соответствующими базовыми значениями аналога или расчетного ПС, принимаемого за эталонный образец. В качестве аналогов выбираются реально существующие ПС того же функционального назначения, что и сравниваемое, с такими же основными параметрами, подобной структуры и применяемые в условиях эксплуатации.

На последнем этапе дается оценка технологической безопасности ПС. Общая оценка качества ПС в целом формируется экспертами по набору полученных значений оценок факторов надежности.

Таким образом, в ходе исследования была предложена методика для оценки технологи-

ческой безопасности ПС. Совокупность расчетных элементов метрик и метрик, вычисляемых методом экспертного опроса, позволяют оценить надежность ПС на стадии эксплуатации и технической поддержки. Это, безусловно, поможет снизить риски, связанные с отказом программного обеспечения на ранней стадии эксплуатации. Зачастую, данная оценка требуется значительно раньше, еще на стадии проектирования. Поэтому предложенная методика будет дорабатываться с целью охвата всех стадий разработки ПО.

Примечания

1. Сводный отчет по безопасности программного обеспечения в России и мире. М.:НПО «Эшелон», 2012. Вып.2. -URL: http://cnpo.ru/report_echelon_2012.pdf.

2. Gallaher M. P. and Kropp B. M. Economic impacts of inadequate infrastructure for software testing. Technical report, RTI International, National Institute of Standards and Technology, US Dept of Commerce, May 2002.

3. Forrest Shull, Vic Basili, Barry Boehm, Winsor A. Brown, Patricia Costa, Mikael Lindvall, Dan Port, Ioana Rus, Roseanne Tesoriero, and Marvin Zelkowitz. What we have learned about fighting defects. In International Software Metrics Symposium. Ottawa, Canada, 2002

4. Марков А.С. Немонотонные модели оценки надежности и безопасности функционирования программных средств на ранних этапах испытаний // Вопросы кибербезопасности. 2014. №2 (3).

5. Goel A. L., Okumoto K. Time-dependent error-detection rate model for software reliability and other performance measures //IEEE transactions on Reliability. – 1979. – Т. 28. – №. 3. – С. 206-211.

6. Patel D. Software Reliability: Models //International Journal of Computer Applications. – 2016. – Т. 152. – №. 9.

Югансон Андрей Николаевич, аспирант, ассистент кафедры проектирования и безопасности компьютерных систем, Университет ИТМО, 197101, г. Санкт-Петербург, Кронверкский проспект, д. 49. E-mail: a_yougunson@corp.ifmo.ru

Заколдаев Данил Анатольевич, кандидат технических наук, доцент, заведующий кафедры проектирования и безопасности компьютерных систем, Университет ИТМО.
197101, г. Санкт-Петербург, Кронверкский проспект, д. 49. E-mail: d.zakoldaev@mail.ru

Iuganson Andrei, PhD student, assistant of Department of Computer System Design and Security, ITMO University.
bld. 49, Kronverkskiy avenue, Saint-Petersburg, 197101, E-mail: a_yougunson@corp.ifmo.ru

Zakoldaev Danil, PhD in Technical Science, associate professor, head of Department of Computer System Design and Security, ITMO University.
bld. 49, Kronverkskiy avenue, Saint-Petersburg, 197101 E-mail: d.zakoldaev@mail.ru