ОЦЕНКА ГАРАНТИРОВАННОСТИ СРЕДСТВ ИНФОРМАЦИОННОГО ОБМЕНА НА ОСНОВЕ ДАННЫХ ТЕСТИРОВАНИЯ

В.В. Соловьёв;
А.С. Крутолапов, доктор технических наук, доцент;
Г.К. Ивахнюк, доктор химических наук, профессор.
Санкт-Петербургский университет ГПС МЧС России

Приведен алгоритм оценки гарантированности средств информационного обмена, основанный на обработке данных по их непосредственному тестированию. Понятие гарантированности связывается с тем, что достигаются необходимые функциональность (целевая пригодность средств информационного обмена) и ее устойчивость (степень надежности и достоверности передаваемых данных).

Ключевые слова: средства информационного обмена, тестирование, гарантированность, набор входных данных, вероятность функционирования, нижняя гарантированная граница, доверительный уровень

WARRANTY ASSESSMENT OF INFORMATION EXCHANGE MEANS ON THE BASIS OF TEST DATA

V.V. Soloviev; A.S. Krutolapov; G.K. Ivakhniuk.
Saint-Petersburg university of State fire service of EMERCOM of Russia

The article describes the algorithm of Warranty assessment of information exchange means based on data of their direct testing. The concept of the warranty associated with the fact that the necessary functionality (target suitability of information exchange means) and its stability (reliability and validity of transmitted data) achieved.

Keywords: information exchange means, testing, warranty, a set of input data, operation probability, lower guaranteed limit, confidence level

В современных условиях наблюдается увеличение сложности и многофункциональности инженерно-технических систем объектов, защиту которых обеспечивают подразделения МЧС России. В этих условиях широкое применение нашли автоматизированные системы диспетчерского управления, характеризующиеся применением передовых информационных технологий при управлении системами пожарной безопасности. Подобные системы построены с использование средств информационного обмена (СИО), надежное функционирование которых предполагает серию прогонов и анализ их результатов для выявления факта наличия или отсутствия логических ошибок [1].

Однако диагностирование взаимодействия компонентов затронуто относительно слабо. Диагностирование взаимодействия модулей – более сложная задача, чем диагностирование самих модулей. Необходимо отметить, что все логические ошибки в СИО полностью выявить и устранить не удается. Поэтому должны быть устранены те ошибки, которые принципиально влияют на их работоспособность.

Между тем обращают на себя внимание следующие аспекты:

1) СИО используются в корпоративных сетях предприятий, где наблюдается большая сложность взаимодействия их элементов. При этом значительное число отказов сетей передачи данных (СПД) (35–40 %) связано с отсутствием должного внимания к вопросам диагностирования взаимодействия модулей.

2) При производстве больших цифровых вычислительных машин в состав операционных систем входит семейство протоколов, которые обеспечивают управление ресурсами. Даже одиночные сбои в их функционировании могут привести к «катастрофическим» последствиям (тупиковым состояниям, зависаниям, блокировкам, переполнению буферов оперативной памяти, полному отказу). На этапе научно-исследовательских и опытно-конструкторских работ (НИОКР) не всегда удается устранить логические ошибки взаимодействия процессов и их несанкционированные прерывания. Для этого предусматривается использование всего арсенала испытаний – периодических, типовых, приемо-сдаточных, направленных на устранение логических ошибок взаимодействия протокольных объектов.

3) Диагностирование СИО широко используется при создании макетных и опытно-промышленных образцов на этапах НИОКР, например, для предотвращения несанкционированных прерываний взаимодействия протокольных объектов в протоколах безопасности.

4) В современных рыночных условиях жесткая конкуренция вынуждает рассматривать возможности злонамеренных воздействий на функционирование защищенных процессов информационного обмена. Защита от вредоносного воздействия злоумышленников в процессе эксплуатации требует диагностирования правильности передачи информации и управления между взаимодействующими модулями для предотвращения несанкционированного доступа к процессам информационного обмена и обнаружения фактов атак на протоколы и алгоритмы.

Указанные обстоятельства обусловливают актуальность исследования моделирования процессов взаимодействия протокольных объектов в СИО.

При этом выбор методов и средств автоматизации зависит от класса создаваемых СИО, требующегося качества, доступных ресурсов на разработку. Ограниченные ресурсы на диагностирование требуют упорядочения методов и рационализации использования средств автоматизации, поэтому диагностирование должно проходить ряд этапов, охватывающих все компоненты СИО с учетом реальных условий (рис. 1).

Тестовые прогоны выполняются на входных наборах данных, выбранных не случайным, а вполне определенным образом. Обычно соответствующий выбор производится так, чтобы найти ошибку быстро и основывается на опыте и интуиции испытателей или осуществляется с учетом функциональных возможностей исследуемой системы. Часто контрольные примеры не представительны с точки зрения моделирования реальных условий работы СИО. После возникновения логической ошибки ее причина выявляется и устраняется, что ведет к изменению гарантированности СИО в процессе его проверки [2].

Программа диагностирования должна охватывать как можно больше типов ситуаций обработки, то есть использовать все допустимые пути своего графа передачи управления. Диагностированию подвергаются как отдельные протокольные объекты (модули) СИО, так и средство в целом.

Рис. 1. **Виды тестирования для различных объектов СИО**

В работе предлагается процедура оценки величины гарантированности R, предусматривающая использование результатов тестирования и включающая следующие шаги:

а) определение множества E входных массивов данных;

б) выделение в E подмножеств G_j, связанных с отдельными ветвями СИО;

в) определение для каждого G_j в предполагаемых условиях функционирования значений вероятности P_j;

г) определение подмножества G_j для каждого входного набора данных, используемых в контрольных примерах;

д) выявление проверенных и непроверенных в ходе тестирования сегментов и пар сегментов;

е) определение для каждого j величины $P=a_jP_j$;

ж) вычисление оценки $\overline{R}$ по формуле:

$$\overline{R} = \sum_{j=1}^{k} P'_j ,$$

где k – общее число ветвей СИО.

Параметр a_j определяется по следующим правилам. Если:

– подмножество G_j включает более одного контрольного примера, то принимается a_j=0,99;

– подмножество G_j включает ровно один контрольный пример, то принимается a_j=0,95;

– подмножество G_j не включает ни одного контрольного примера, но в процессе проверки протокола были пройдены все сегментные пары ветви L_j, то принимается a_j=0,90;

– в ходе тестирования были опробованы все сегменты, но не все сегментные пары, то принимается a_j=0,80;

– m сегментов ($1 \le m \le 4$) ветви L_j не были опробованы в ходе тестирования, то принимается a_j=0,80–0,20;

– более чем четыре сегмента не были опробованы в процессе тестирования, то принимается a_j=0.

Для оценки гарантированности логически завершенного СИО предлагается следующий алгоритм.

Вход: логически завершенное СИО, набор входных данных E, разбитый на K подмножеств S_j. Для каждого S_j известно количество проводимых тестов n_j и вероятность обнаружения ошибки P_j при n_j тестах.

Выход: нижняя доверительная граница гарантированности СИО (по Нейману) при заданном доверительном уровне равна γ.

Шаг 1. Ввести K – количество подмножеств S_j множества E. Если K не является допустимым, то информировать об ошибке и потребовать ввести K заново.

Шаг 2. Для каждого S_j ввести количество проводимых тестов n_j. Если n_j не является допустимым, то информировать об ошибке и потребовать ввести n_j заново.

Шаг 3. Для каждого S_j ввести вероятность обнаружения ошибки P_j для n_j проводимых тестов. Если P_j не является допустимым, то информировать об ошибке и потребовать ввести P_j заново.

Шаг 4. Задать доверительный уровень γ. Если γ не является допустимым, то информировать об ошибке и потребовать ввести γ заново.

Шаг 5. Если данные были введены корректно, то рассчитать нижнюю доверительную границу гарантированности СИО R_L.

Основная расчетная формула:

$$R_L = n(1-\gamma)^{\frac{1}{n}} \prod_{j=1}^{K} \left(\frac{P_j}{n_j} \right)^{\frac{n_j}{n}},$$

где $n = \sum_{j=1}^{K} n_j$.

Предложенная методика тестирования реализована в программном средстве анализа достижимых состояний протокола *TCP*.

На основе алгоритма проведено моделирование для нахождения нижних доверительных границ гарантированности СИО. Предположение об асимптотически нормальном поведении СИО не рассматривалось. Результаты моделирования представлены на рис. 2–4. На графике (рис. 2) показано, что линейный участок нижней доверительной границы гарантированности начинается при оптимальном количестве тестов от 7 до 20–21. При дальнейшем увеличении количества прогонов испытаний вероятность (точность) обнаружения логической ошибки в СИО не увеличивается. В расчётах взят доверительный уровень 0,95 и вероятность наличия ошибки в каждом из подмножеств 0,05. На графиках (рис. 3, 4) показаны результаты при проведении 10 тестов. При пропорциональных отношениях количества тестов и вероятности обнаружения ошибки для каждого из подмножеств зависимость нижней доверительной границы гарантированности СИО от вероятности обнаружения ошибки в каждом из подмножеств почти линейная.

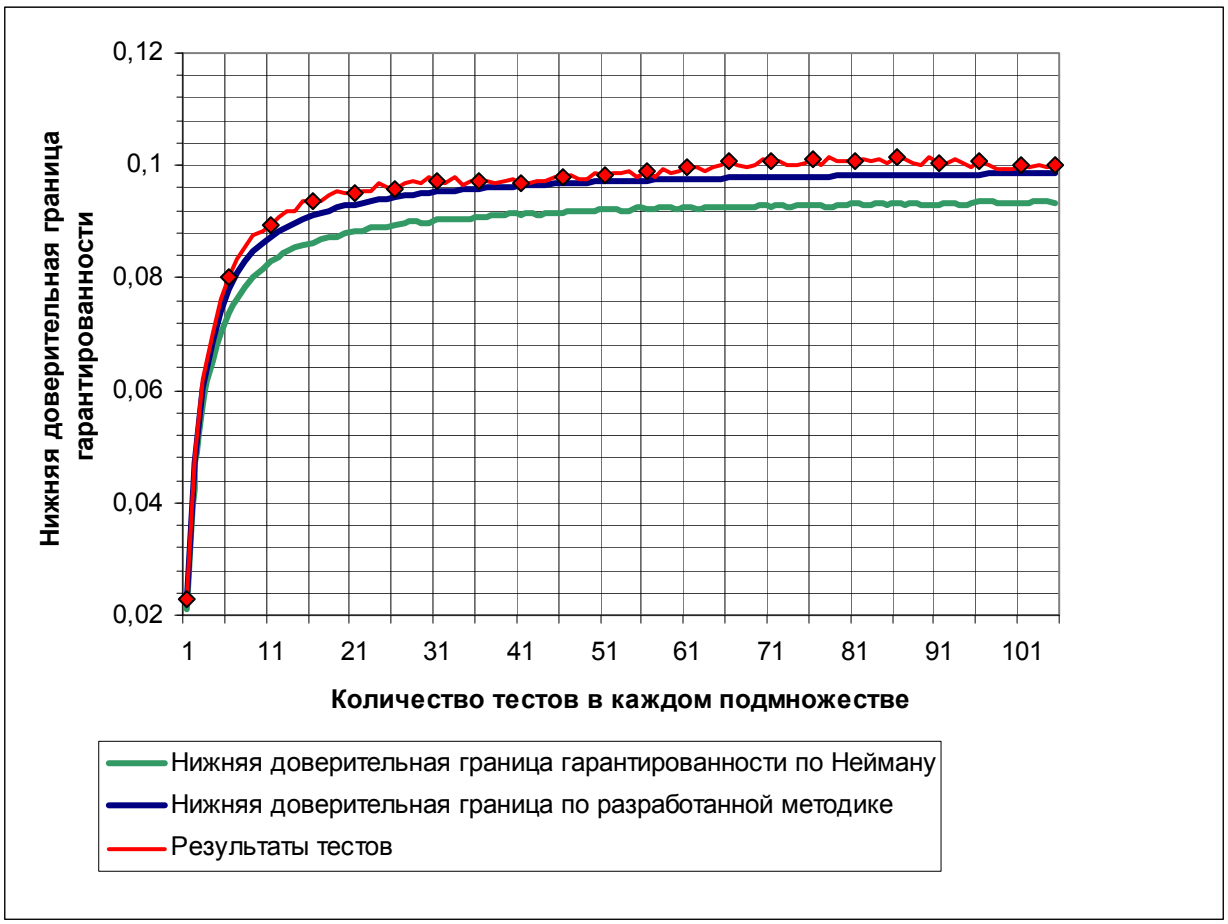

Рис. 2. **Функциональная зависимость нижней доверительной границы допустимой гарантированности средства информационного обмена от количества тестов**

Приведенные выше значения параметра a_j определены на основе анализа теоретических результатов исследования и экспериментальных результатов проверок различных реализаций [3]. Для каких-то специфических программ и специальных процедур их проверки возможно получение лучших оценок значений этих параметров. Для получения более точной оценки величины R необходимо провести измерение надежности с использованием подходящего метода формировании выборки.

Более точное определение гарантированности СИО включает описание некоторой вычисляемой функции F, для выполнения которой предназначено СИО. Обычно эта функция описывается в протокольных спецификациях, но они сами могут содержать ошибки, поэтому функция F определяется в процессе поиска решения конкретной физической задачи, получаемого с помощью данного СИО.

Аналогичный подход может быть применен и к обеспечению гарантированности функционирования СИО при возникновении отказа системы из-за ошибки в протоколе.

Надежность функционирования СИО $S(E_i)$ имеет условие соблюдения ограничения: $F'(E_i) \leq S(E_i)$. Оно может быть введено взамен прежнего условия корректного функционирования СИО. Конкретные условия поведения системы после нарушения ее нормальной работы определяют, приведет ли отказ СИО к нарушению условия надежности.

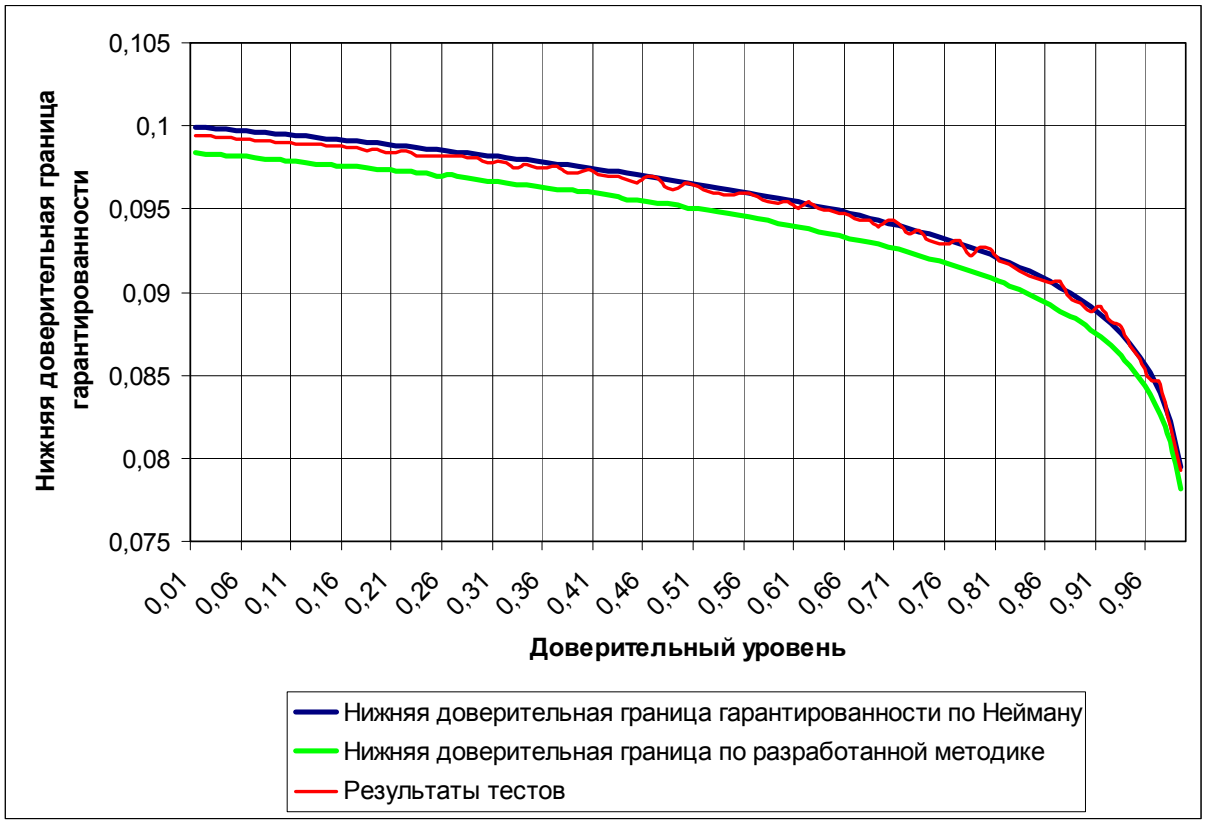

Рис. 3. **Функциональная зависимость нижней доверительной границы гарантированности средства информационного обмена от доверительного уровня**

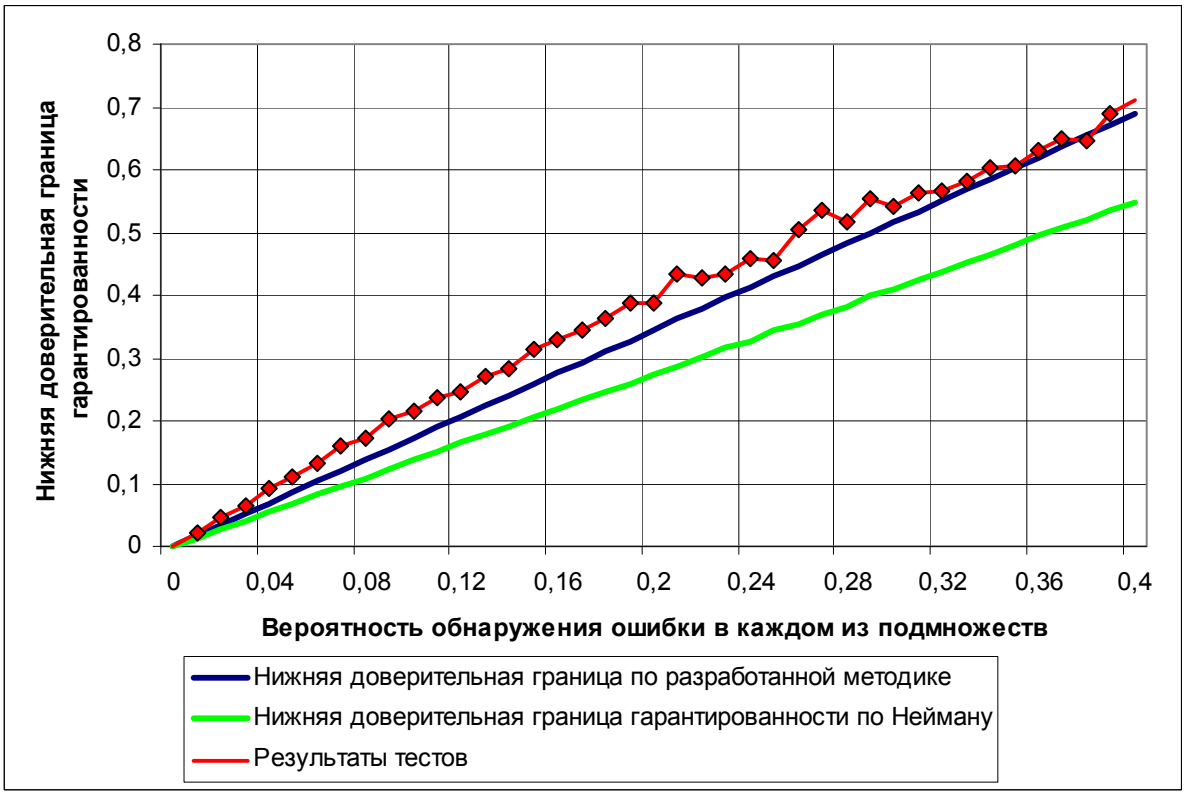

Рис. 4. **Функциональная зависимость нижней доверительной границы допустимой гарантированности средства информационного обмена от вероятности обнаружения ошибки**

Надежность функционирования СИО $S(E_i)$ имеет условие соблюдения ограничения: $F'(E_i) \leq S(E_i)$. Оно может быть введено взамен прежнего условия корректного функционирования СИО. Конкретные условия поведения системы после нарушения ее нормальной работы определяют, приведет ли отказ СИО к нарушению условия надежности.

Введя определение надежного и ненадежного функционирования СИО, можно использовать вышеуказанные формулы для вычисления характеристик устойчивости.

Исправление ошибок и доказательство корректности СИО относятся к процессу верификации. В соответствии с рекомендациями международных и российских стандартов основополагающим критерием пригодности изделия является гарантированность его реализации как вероятность безотказного выполнения предназначенных операций за определенное количество их повторов. Понятие гарантированности связывается с тем, что достигаются необходимые функциональность (целевая пригодность СИО) и устойчивость (степень надежности и достоверности передаваемых данных). В работе приведен пример оценки гарантированности СИО, которая оценивается в результате тестирования.

Литература

1. Крутолапов А.С., Хлобыстин Н.С. Методика обнаружения и коррекции прерываний вне протокола в сетях передачи данных // Научно-технические ведомости СПбГПУ. Сер.: Информатика. Телекоммуникации. Управление. 2012. № 2 (145).

2. Крутолапов А.С., Гадышев В.А., Сычев Д.А. Алгоритм распределения потоков в сетях передачи данных // Системы управления и информационные технологии. 2011. № 4.1 (46).

3. Абрамян Г.А., Крутолапов А.С., Одоевский С.М. Модель обеспечения качества обслуживания в сетях передачи данных // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2011. № 4. С. 36–41.