УДК 004.05+004.415.5

Ю.С. МАНЖОС, В.Л. ПЕТРИК

Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина

ОЦЕНКА ПОЛНОТЫ СЕМАНТИЧЕСКОГО КОНТРОЛЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Исследована степень полноты семантического контроля программного обеспечения информационно-управляющих систем авиационно-космических комплексов, основанного на анализе использования физических размерностей. Разработаны и проанализированы модели полноты семантического контроля программного обеспечения. Доказана устойчивость полученных результатов.

семантический контроль программного обеспечения, полнота семантического контроля, статистические характеристики программного обеспечения

Введение

Независимая верификация (НВ) программного обеспечения (ПО) информационно-управляющих систем (ИУС) авиационно-космических комплексов, выполняемая сертификационными центрами, возможна посредством формального доказательства корректности, основанного на использовании семантического контроля. Достоверность НВ снижается ввиду неполноты контроля всех функциональных свойств, неполноты документирования ПО либо невозможности ввода всех семантических характеристик в условиях ограниченных ресурсов сертификационных центров [1 – 7]. Это требует уточнения оценки полноты, являющейся важным фактором достоверности НВ.

В общем случае полнота контроля исходного программного кода может быть оценена на основе анализа статистических характеристик посредством анализа динамической модели семантической полноты [2].

Постановка задачи. Целью данной статьи является оценка полноты семантического контроля (СК) ПО, основанного на анализе корректности использования физических размерностей, и влияния на достоверность оценки доли документированных программных переменных.

Это потребует решения следующих задач:

1) анализ статистических характеристик реального программного кода и обоснование использования методов теории случайных процессов.

2) разработка и анализ модели полноты семантического контроля ПО ИУС.

3) анализ устойчивости решения.

1. Анализ статистических характеристик реального программного кода и обоснование использования методов теории случайных процессов

Необходимым условием применения методов теории случайных процессов для анализа полноты является пуассоновский характер распределения операций и операндов. Для анализа законов статистических распределений использовался статический анализатор (СА).

Большинство операций можно отнести к *аддитивным: "сложение"*, *"вычитание"*, *"присваивание"*, *"сравнение"*, которые не формируют новых семантик (физических размерностей) и используются только для контроля совпадения размерностей операндов; и *мультипликативным: "умножение"*, *"деление"*, *"возведение в степень"*, которые порождают новые семантики и не контролируют размерности своих аргументов. Кроме того, имеется неко-

торая часть операций, реализующих условные и безусловные переходы, а также логические.

Появление операций в программном коде можно рассматривать как некоторое случайное событие. Поток операций обладает определенными свойствами: *ординарностью,* так как операции появляются поодиночке и вероятность попадания на элементарный участок кода двух или более операций гораздо ниже вероятности попадания на него ровно одной операции; *отсутствием последействия*, так как для любых неперекрывающихся участков кода количество операций является независимыми случайными величинами, т.е. вероятность попадания любого количества операций не зависит от того, сколько их попало на другие; *стационарностью*, так как вероятностные характеристики не меняются в адресном пространстве программного кода, и вероятность попадания определенного количества операций на участок кода зависит только от длины участка и не зависит от расположения.

Вследствие того, что поток операций обладает свойствами *ординарности*, *стационарности* и *отсутствия последействия,* он является простейшим или стационарным пуассоновским потоком, что позволяет для исследования свойств программного кода использовать методы теории случайных процессов [8], применение которых обуславливает необходимость определения статистических характеристик – интенсивностей операций.

Результаты анализа программного кода показаны на рис. 1. Например, значению абсциссы 6 соответствует 200 для аддитивных операций, т.е. в программном коде найдено 200 участков, ограниченных аддитивными операциями и содержащих 5 иных операций. Аналогично найдено 1600 интервалов, ограниченных аддитивными операциями, содержащими внутри 3 неаддитивных операции.

В дальнейшем вычисляются относительные интенсивности появления операций, графики которых показаны на рис. 2. Интегральным инвариантом операционного потока является единичная сумма площадей под кривыми относительных интенсивностей операций.

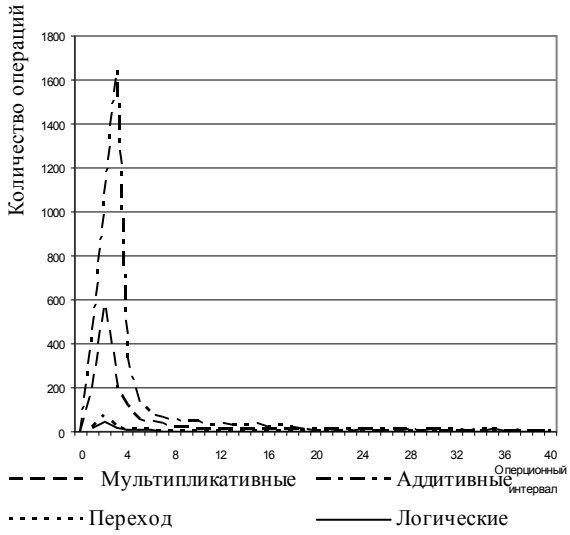

Рис. 1. Абсолютные интенсивности операций

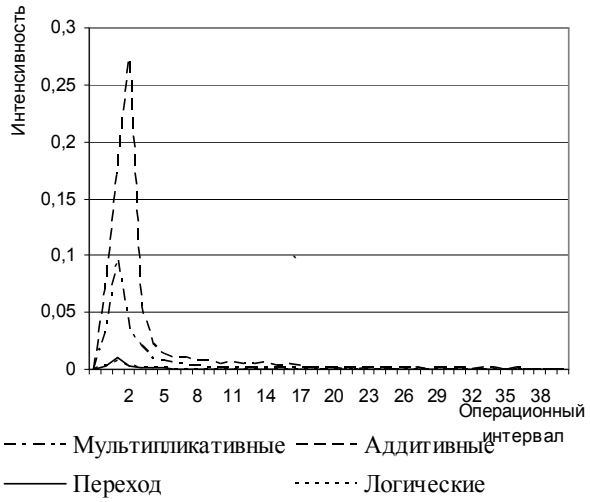

Рис. 2. Относительные интенсивности операций

2. Разработка и анализ модели полноты семантического контроля программного обеспечения информационно-управляющих систем

Достоверность оценки корректности, получаемой контролем семантических инвариантов посредством СА определяется неполнотой контроля всех функциональных свойств ПО, неполнотой документированности, невозможностью контроля логии-

ческих операций, а также наличием большого количества безразмерных переменных.

В общем случае полнота может быть оценена с помощью коэффициента семантической полноты (КСП) как:

$$\Omega = \frac{P_F}{P_F + P_{\overline{F}}}, \qquad (1)$$

где P_F, $P_{\overline{F}}$ – вероятности обнаружения и необнаружения семантических дефектов (СД) при условии их существования.

В соответствии с семантической алгеброй [6] обнаружение СД возможно для аддитивных, мультипликативных операций и операций сравнения. При этом вызов программных функций может быть отнесен к аддитивным операциям вследствие возможности контроля семантик формально-фактических параметров. В тоже время логические операции и операции перехода не контролируются.

Для нахождения КСП удобно работу СА представить в виде модели, граф которой, отражающий возможные состояния СА, переходы между ними, а также вероятности переходов, показан на рис. 3.

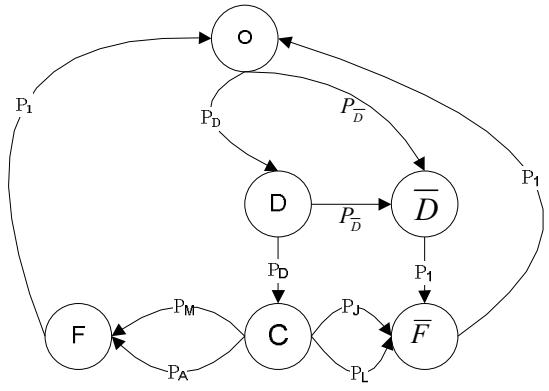

Рис. 3. Полная дискретная модель состояний

Предполагается, что первоначально СА находится в состоянии O – операнд, а операнды с вероятностью могут быть P_D документированы и с вероятностью $P_{\overline{D}} = 1 - P_D$ недокументированы. Эти вероятности определяют переходы СА в состояния D – «документированный операнд» и $\overline{D}$ – «недокументированный операнд». При появлении недокументированного операнда СА переходит в состояние $\overline{D}$, в котором идентификация СД невозможна, поэтому СА из этого состояния с единичной вероятностью переходит в состояние $\overline{F}$ – «невозможность обнаружения нарушений СД», а далее с единичной вероятностью возвращается в начальное состояние O.

При переходе СА в состояние D – «документированный операнд» в зависимости от документированности второго операнда бинарной операции СА с соответствующей вероятностью переходит либо в состояние C – «команда», либо в состояние $\overline{D}$. При переходе СА в состояние «команда» в зависимости от типа исполняемой команды с суммарной вероятностью P_A (аддитивные операции) + P_M (мультипликативные операции) осуществляется переход в состояние F – «возможность обнаружения нарушений СД», а с суммарной вероятностью P_J (операции перехода) + P_L (логические операции) переход в состояние $\overline{F}$.

В связи с единичной вероятностью перехода из состояния $\overline{D}$ в состояние $\overline{F}$, эти узлы можно объединить. В результате получим упрощенную модель (рис. 4), в которой состояния O_1, O_2 соответствуют первому и второму операнду.

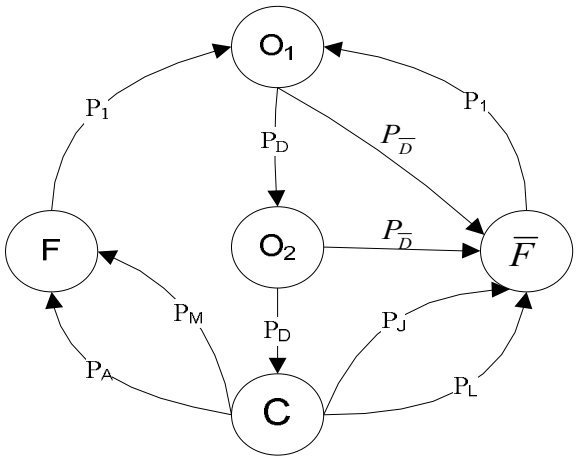

Рис. 4. Упрощенная дискретная модель состояний

Упрощенная дискретная модель позволяет записать систему линейных алгебраических уравнений

(СЛАУ), описывающих потоки вероятностей для каждого из пяти узлов.

$$\begin{cases} S_{O1}(P_D + P_{\overline{D}}) = S_{\overline{F}}P_1 + S_F P_1; \\ S_{O2}(P_D + P_{\overline{D}}) = S_{O1}P_D; \\ S_{\overline{F}}P_1 = S_{O1}P_{\overline{D}} + S_{O2}P_{\overline{D}} + S_C(P_L + P_J); \\ S_C(P_A + P_M + P_L + P_J) = S_{O2}P_D; \\ S_F P_1 = S_C(P_A + P_M), \end{cases} \quad (2)$$

где $S_{O1}, S_{O2}, S_{\overline{F}}, S_F, S_C$ – искомые вероятности нахождения СА в каждом из состояний, а $P_D, P_{\overline{D}}, P_A, P_J, P_L, P_M$ – переходные вероятности.

Необходимым условием, которому должно удовлетворять решение, является уравнение нормировки:

$$S_{O1} + S_{O2} + S_{\overline{F}} + S_F + S_C = 1. \quad (3)$$

Система (2) имеет пять неизвестных, поэтому любое из уравнений, например третье, можно исключить, заменив нормировочным условием.

Переходные вероятности также образуют полные группы событий, поэтому $P_D + P_{\overline{D}} = 1$ и $P_A + P_M + P_L + P_J = 1$. Отсюда:

$$\begin{cases} S_{O1} = S_{\overline{F}} + S_F; \\ S_{O2} = S_{O1}P_D; \\ S_C = S_{O2}P_D; \\ S_F = S_C(P_A + P_M); \\ S_{O1} + S_{O2} + S_{\overline{F}} + S_F + S_C = 1. \end{cases} \quad (4)$$

Для нахождения КСП подставим в выражение (1) значения вероятностей нахождения СА в соответствующих узлах $S_{\overline{F}}$ и S_F, которые соответствуют $P_{\overline{F}}$, P_F – вероятностям необнаружения и обнаружения СД при условии их существования. Подставив в знаменатель (1) первое уравнение системы (4), а в числитель – значение из четвертого, получим:

$$\Omega = \frac{S_C(P_A + P_M)}{S_{O1}}. \quad (5)$$

После подстановки из третьего уравнения системы (4) имеем:

$$\Omega = \frac{S_{O2}P_D(P_A + P_M)}{S_{O1}}. \quad (6)$$

Подставив из второго уравнения системы (4) в (6) значение S_{O2}, имеем искомое значение КСП:

$$\Omega = \frac{S_{O1}P_D P_D(P_A + P_M)}{S_{O1}} = P_D^2(P_A + P_M). \quad (7)$$

Вернемся к полной дискретной модели, представленной на рис. 3. Система уравнений, описывающая потоки вероятностей и условие нормировки имеет вид:

$$\begin{cases} S_O(P_D + P_{\overline{D}}) = S_{\overline{F}}P_1 + S_F P_1; \\ S_D(P_D + P_{\overline{D}}) = S_O P_D; \\ S_{\overline{D}}P_1 = S_O P_{\overline{D}} + S_D P_{\overline{D}}; \\ S_C(P_A + P_M + P_L + P_J) = S_D P_D; \\ S_{\overline{F}}P_1 = S_{\overline{D}}P_1 + S_C(P_L + P_J); \\ S_F P_1 = S_C(P_A + P_M); \\ S_O + S_D + S_{\overline{D}} + S_{\overline{F}} + S_F + S_C = 1. \end{cases} \quad (8)$$

Неизвестных $S_O, S_D, S_{\overline{D}}, S_{\overline{F}}, S_F, S_C$ шесть, любое уравнение, кроме нормировочного (седьмое уравнение системы (8)), можно исключить. Модифицированная система:

$$\begin{cases} S_O = S_{\overline{F}} + S_F; \\ S_D = S_O P_D; \\ S_{\overline{D}} = P_{\overline{D}}(S_O + S_D); \\ S_{\overline{F}} = S_{\overline{D}} + S_C(P_L + P_J); \\ S_F = S_C(P_A + P_M); \\ S_O + S_D + S_{\overline{D}} + S_{\overline{F}} + S_F + S_C = 1. \end{cases} \quad (9)$$

КСП, выраженный через вероятности нахождения СА в узлах модели:

$$\Omega = \frac{S_F}{S_F + S_{\overline{F}}}. \quad (10)$$

Решая систему (9) и подставляя значения вероятностей в (10), получим КСП:

$$\Omega = (P_A + P_M)P_D^2. \quad (11)$$

Рассмотрим далее модель с непрерывными состояниями, отличающуюся от полной дискретной модели использованием не переходных вероятностей, а интенсивностей (рис. 5). Основанием для использования непрерывной модели является большой объем программного кода, позволяющий рассматривать процесс статического анализа как непрерывный процесс.

Предполагается, что первоначально СА находится в состоянии O – операнд, причем семантически документированные операнды появляются с интенсивностью λ_D, а недокументированные – с интенсивностью $\lambda_{\overline{D}}$ и переводят СА в состояния D – «документированный операнд», после которого возможна идентификация СД, и в состояние $\overline{D}$ – «недокументированный операнд», после которого идентификация СД невозможна, поэтому СА с единичной вероятностью переходит в состояние $\overline{F}$ – «невозможность обнаружения нарушений СД», а далее безусловно возвращается в состояние O.

При переходе в состояние D СА с интенсивностью $\lambda_{\overline{D}}$ переходит в состояние $\overline{D}$, а с интенсивностью λ_D в состояние C – «команда». При переходе СА в состояние C в зависимости от типа исполняемой команды с суммарной интенсивностью P_A (аддитивные операции) + P_M (мультипликативные операции) осуществляется переход в состояние F – «возможность обнаружения нарушений СД», а с суммарной интенсивностью P_J (операции перехода) + P_L (логические операции) переход в состояние $\overline{F}$, из которого возвращается состояние O.

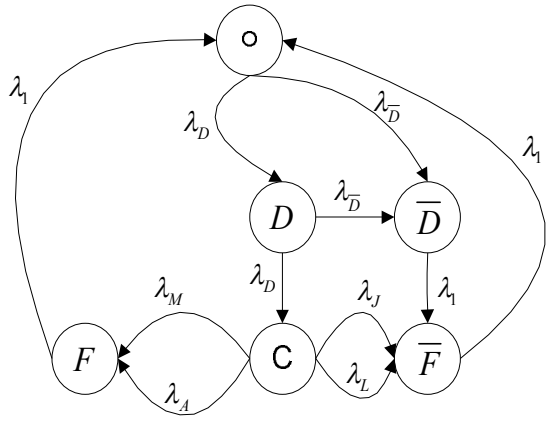

Рис. 5. Непрерывная модель полноты контроля

Полная непрерывная модель позволяет определить систему дифференциальных уравнений (СДУ) Колмогорова (12), связывающих потоки вероятностей в каждом из состояний с изменениями вероятностей нахождения СА в этих состояниях (производными):

$$\begin{cases} \dfrac{dP_O}{dt} = P_F\lambda + P_{\overline{F}}\lambda - P_O(\lambda_D + \lambda_{\overline{D}}); \\ \dfrac{dP_D}{dt} = P_O\lambda_D - P_D(\lambda_D + \lambda_{\overline{D}}); \\ \dfrac{dP_{\overline{D}}}{dt} = P_O\lambda_{\overline{D}} + P_D\lambda_{\overline{D}} - P_{\overline{D}}\lambda_1; \\ \dfrac{dP_{\overline{F}}}{dt} = P_C\lambda_L + P_C\lambda_J + P_{\overline{D}}\lambda_1 - P_{\overline{F}}\lambda_1; \\ \dfrac{dP_C}{dt} = P_D\lambda_D - P_C(\lambda_L + \lambda_M + \lambda_J + \lambda_A); \\ \dfrac{dP_F}{dt} = P_C(\lambda_M + \lambda_A) - P_F\lambda_1. \end{cases} \quad (12)$$

Следует отметить, что модель является динамической, а сами вероятности нахождения СА в каждом из состояний имеют некоторые пределы. Для нахождения значений предельных вероятностей, а значит и предела

$$\lim_{t\to\infty}\Omega = \frac{\lim\limits_{t\to\infty} P_F}{\lim\limits_{t\to\infty} P_F + \lim\limits_{t\to\infty}\overline{F}},$$

где t – номер анализируемого операнда, приравняем значения производных нулю и получим СЛАУ, описывающих асимптоты вероятностей нахождения СА в узлах:

$$\begin{cases} P_F\lambda + P_{\overline{F}}\lambda - P_O(\lambda_D + \lambda_{\overline{D}}) = 0; \\ P_O\lambda_D - P_D(\lambda_D + \lambda_{\overline{D}}) = 0; \\ P_O\lambda_D + P_D\lambda_{\overline{D}} - P_{\overline{D}}\lambda_1 = 0; \\ P_C\lambda_L + P_C\lambda_J + P_{\overline{D}}\lambda_1 - P_{\overline{F}}\lambda_1 = 0; \\ P_D\lambda_D - P_C(\lambda_L + \lambda_M + \lambda_J + \lambda_A) = 0; \\ P_C(\lambda_M + \lambda_A) - P_F\lambda_1 = 0. \end{cases} \quad (13)$$

Одно из уравнений является избыточным и на основании условия нормировки должно быть заменено на алгебраическое уравнение:

$$P_O + P_D + P_{\overline{D}} + P_C + P_F + P_{\overline{F}} = 1. \quad (14)$$

Решение системы (13) с учетом (14) имеет вид:

$$\Omega = \lambda_D^2 \frac{(\lambda_M + \lambda_A)}{(\lambda_D + \lambda_{\overline{D}})^2(\lambda_L + \lambda_M + \lambda_J + \lambda_A)}, \quad (15)$$

который практически совпадает с (7). В соответствии с обозначениями: λ_D, $\lambda_{\overline{D}}$ – интенсивности

появления в коде документированных и недокументированных переменных, т.е. переменных, имеющих известные семантики; $\lambda_L, \lambda_M, \lambda_J, \lambda_A$ – интенсивности появления логических операций, мультипликативных операций, переходов и аддитивных операций. Общая сумма интенсивностей их появления равна 1.

Обозначив долю семантически контролируемых операций $k = \frac{(\lambda_M + \lambda_A)}{(\lambda_L + \lambda_M + \lambda_J + \lambda_A)}$, отобразим на рис. 6 значения коэффициента семантической полноты.

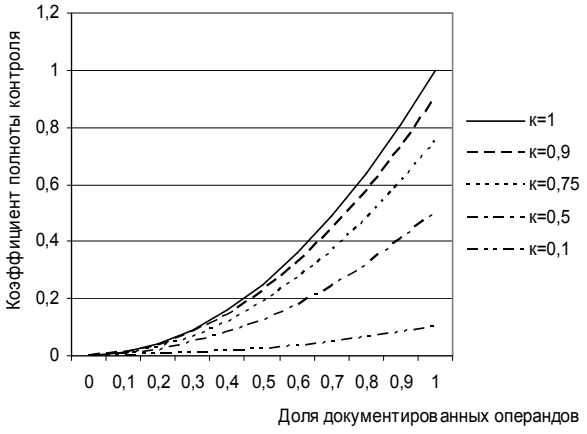

Рис. 6. Зависимость коэффициента семантической полноты контроля от уровня документированности

3. Анализ устойчивости решения

Практическую ценность полученных результатов необходимо подтвердить, доказав устойчивость полученного решения [9]. Это вызвано тем, что коэффициенты СДУ (12) определяются на основе статистических исследований, поэтому необходимо оценить влияние погрешностей их значений на окончательный результат.

Непосредственное аналитическое доказательство устойчивости СДУ (12) невозможно ввиду высокого порядка системы и степени соответствующего ей характеристического уравнения. Для упрощения выкладок преобразуем граф полной непрерывной модели, показанный на рис. 5, к эквивалентному виду, показанному на рис. 7.

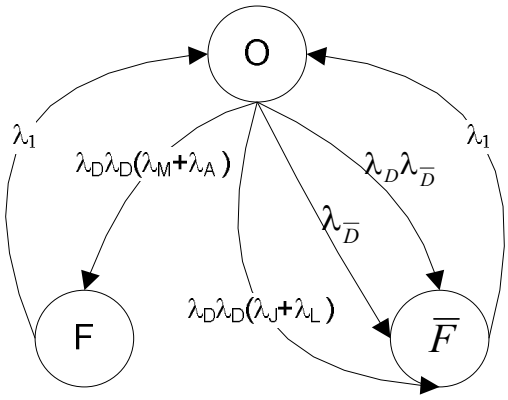

Рис. 7. Приведенная полная непрерывная модель полноты семантического контроля

Приведенной модели соответствует следующая СДУ Колмогорова:

$$\begin{cases} \dot{P}_O = P_F\lambda_1 + P_{\overline{F}}\lambda_1 - P_O(\lambda_D^2(\lambda_M + \lambda_A) + \\ + \lambda_D^2(\lambda_J + \lambda_L) + \lambda_{\overline{D}} + \lambda_D\lambda_{\overline{D}}); \\ \dot{P}_F = P_O\lambda_D^2(\lambda_M + \lambda_A) - P_F\lambda_1; \\ \dot{P}_{\overline{F}} = P_O(\lambda_{\overline{D}} + \lambda_D\lambda_{\overline{D}} + \lambda_D^2(\lambda_J + \lambda_L)) - P_{\overline{F}}\lambda_1. \end{cases} \quad (16)$$

Т.к. $\lambda_D + \lambda_{\overline{D}} = 1$ и $\lambda_A + \lambda_R + \lambda_L + \lambda_J = 1$, то

$$\begin{cases} \dot{P}_O = -P_O(\lambda_D^2(\lambda_M + \lambda_A) + \lambda_D^2(\lambda_J + \lambda_L) + \\ + \lambda_{\overline{D}} + \lambda_D\lambda_{\overline{D}}) + P_F\lambda_1 + P_{\overline{F}}\lambda_1; \\ \dot{P}_F = P_O\lambda_D^2(\lambda_M + \lambda_A) - P_F\lambda_1; \\ \dot{P}_{\overline{F}} = P_O(\lambda_{\overline{D}} + \lambda_D\lambda_{\overline{D}} + \lambda_D^2(\lambda_J + \lambda_L)) - P_{\overline{F}}\lambda_1. \end{cases} \quad (17)$$

Преобразуем СДУ (17) в линейную систему с постоянными коэффициентами.

Введем обозначения:

$$\begin{cases} a_O = -(\lambda_D^2(\lambda_M + \lambda_A) + \lambda_D^2(\lambda_J + \lambda_L) + \\ + \lambda_{\overline{D}} + \lambda_D\lambda_{\overline{D}}); \\ a_F = \lambda_D^2(\lambda_M + \lambda_A); \\ a_{\overline{F}} = \lambda_{\overline{D}} + \lambda_D\lambda_{\overline{D}} + \lambda_D^2(\lambda_J + \lambda_L). \end{cases}$$

Тогда система (17) примет вид:

$$\begin{cases} \dot{P}_O = a_O P_O + 1P_F + 1P_{\overline{F}}; \\ \dot{P}_F = a_F P_O - 1P_F + 0P_{\overline{F}}; \\ \dot{P}_{\overline{F}} = a_{\overline{F}} P_O + 0P_F - 1P_{\overline{F}}. \end{cases} \quad (18)$$

Обозначив общую интенсивность семантически контролируемых операций $\lambda_C = \lambda_M + \lambda_A$, а неконтролируемых операций $\lambda_{\overline{C}} = \lambda_J + \lambda_L$ и принимая

во внимание, что $\lambda_C + \lambda_{\overline{C}} = 1$, имеем:

$$\begin{cases} a_O = -(\lambda_D^2 + (1-\lambda_D) + \lambda_D(1-\lambda_D); \\ a_F = \lambda_D^2 \lambda_C; \\ a_{\overline{F}} = (1-\lambda_D) + \lambda_D(1-\lambda_D) + \lambda_D^2(1-\lambda_C). \end{cases}$$

После преобразований получаем, что

$$\begin{cases} a_O = -(\lambda_D^2 + 1 - \lambda_D + \lambda_D - \lambda_D^2) = -1; \\ a_F = \lambda_D^2 \lambda_C; \\ a_{\overline{F}} = 1 - \lambda_C \lambda_D^2. \end{cases}$$

Окончательно:

$$\begin{cases} a_O = -1; \\ a_F = \lambda_D^2 \lambda_C; \\ a_{\overline{F}} = 1 - \lambda_D^2 \lambda_C. \end{cases} \quad (19)$$

Отбросив первое уравнение системы (18) и выразив P_O из $P_O + P_F + P_{\overline{F}} = 1$, получим, после подстановки во второе и третье уравнения системы (18) систему алгебро-дифференциальных уравнений:

$$\begin{cases} \dot{P}_F = a_F(1 - P_F - P_{\overline{F}}) - 1P_F + 0P_{\overline{F}}; \\ \dot{P}_{\overline{F}} = a_{\overline{F}}(1 - P_F - P_{\overline{F}}) + 0P_F - 1P_{\overline{F}}, \end{cases} \quad (20)$$

которая приводится к СДУ:

$$\begin{cases} \dot{P}_F = a_F - a_F P_F - a_F P_{\overline{F}} - P_F + 0P_{\overline{F}}; \\ \dot{P}_{\overline{F}} = a_{\overline{F}} - a_{\overline{F}} P_F - a_{\overline{F}} P_{\overline{F}} + 0P_F - 1P_{\overline{F}}. \end{cases} \quad (21)$$

Получаем линейную однородную СДУ с действительными постоянными коэффициентами:

$$\begin{cases} \dot{P}_F = -(a_F + 1)P_F - a_F P_{\overline{F}} + a_F; \\ \dot{P}_{\overline{F}} = -a_{\overline{F}} P_F - (a_{\overline{F}} + 1)P_{\overline{F}} + a_{\overline{F}}, \end{cases} \quad (22)$$

частные решения которой будем искать в виде:

$$\begin{cases} P_F = \alpha_1 e^{kt}; \\ P_{\overline{F}} = \alpha_2 e^{kt}, \end{cases} \quad (23)$$

где α_1, α_2, k – постоянные.

Подставляя (23) в (22) и сокращая на e^{kt}, получим для определения α_1, α_2 СЛАУ:

$$\begin{cases} (-(a_F + 1) - k)\alpha_1 - a_F \alpha_2 = 0; \\ -a_{\overline{F}} \alpha_1 + (-(a_{\overline{F}} + 1) - k)\alpha_2 = 0. \end{cases} \quad (24)$$

Наличие нетривиального решения системы (24) требует равенства нулю определителя:

$$\begin{vmatrix} -(a_F + 1) - k & -a_F \\ -a_{\overline{F}} & -(a_{\overline{F}} + 1) - k \end{vmatrix} = 0. \quad (25)$$

Условием устойчивости системы (22) является отрицательность корней характеристического уравнения, получаемого из (25):

$$(-a_F - 1 - k)(-a_{\overline{F}} - 1 - k) - a_F a_{\overline{F}} = 0. \quad (26)$$

Уравнение (26) с учетом (19) приводится к квадратному уравнению $k^2 + 3k + 2 = 0$, корни которого $k_1 = -2$ и $k_2 = -1$.

Таким образом, оба корня характеристического уравнения (26) отрицательны. Все решения асимптотически устойчивы в целом по показательному закону, что позволяет использовать полученный результат (15) для оценки полноты семантической проверки исходного кода информационно-управляющих систем критического применения посредством статического анализа.

Заключение

Показано, что применение статического анализа для СК исходного кода ПО позволяет достичь в среднем только 30% покрытия, а сам коэффициент покрытия пропорционален квадрату доли документированных переменных и зависит от доли неконтролируемых операций. Доказана устойчивость полученного решения.

Таким образом, получаем естественный результат: чем выше доля документированных переменных, тем выше уровень контроля, который в пределе достигает единицы. Однако, при слабой документированности ПО, когда доля документированных переменных составляет около 0,1, достигаемая полнота 0,01. Двукратное увеличение документированности позволяет достичь покрытия только 0,04 исходного кода.

Дальнейшее повышение полноты при отсутствии детальной документации либо при ресурсных ограничениях, не позволяющих вводить семантики всех известных программных переменных, возможно

посредством решения систем линейных алгебраических уравнений, построенных на основе семантической алгебры и известных семантик программных переменных. При этом каждой аддитивной операции будет соответствовать свое алгебраическое уравнение, что позволит довести уровень документированности и полноту семантического контроля программного обеспечения до 100%.

Литература

1. Харченко В.С., Манжос Ю.С., Петрик В.Л. Статистический анализ программного обеспечения системы управления космическим аппаратом и оценка проверяющей способности семантического контроля // Технология приборостроения. – 2002. – № 2. – С. 52–59.

2. Петрик В.Л. Оценка полноты независимой верификации в условиях неопределенных проектных спецификаций // Міжнародна науково-технічна конференція «Інтегровані комп'ютерні технології в машинобудуванні» ІКТМ'2006: Тези доповідей. – Х.: Нац. аерокосм. ун-т «ХАІ», 2006. – С. 483-484.

3. Манжос Ю.С. Оценка эффективности независимой верификации программного обеспечения // Авиационно-космическая техника и технология. – 2004. – № 7. – С. 210-214.

4. Манжос Ю.С. Типізація даних у системах критичного застосування // Системи обробки інформації. – Х.: ХВУ, 2002. – Вип. 3 (19). – С. 54-57.

5. Манжос Ю.С. Принципы семантического контроля программного обеспечения // Авиационно-космическая техника и технология. – Х.: Нац. аэрокосм. ун-т „Харк. авиац. ин-т", 2002. – Вып. 32. – С. 307-315.

6. Манжос Ю.С. Семантический контроль программного обеспечения систем критического применения // Авиационно-космическая техника и технология. – Х.: Нац. аэрокосм. ун-т „Харк. авиац. ин-т", 2002. – Вип. 34. – С. 207-212.

7. Конорев Б.М., Манжос Ю.С., Харченко В.С., Чертков Г.Н. Семантический метод независимой верификации программного обеспечения информационно-управляющих систем важных для безопасности АЭС // Международный симпозиум «Измерения, важные для безопасности в реакторах». – М.: Институт проблем управления им. Трапезникова, 2003. – С. 10-1–10-14.

8. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. – М.: Наука, 1988. – 480 с.

9. Араманович И.Г., Лунц Г.Л., Эльсгольц Л.Э. Функции комплексного переменного. Операционное исчисление. Теория устойчивости. – М.: Наука, 1965. – 392 с.

Поступила в редакцию 12.09.2007

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков.