УДК 004.05+004.415.5

В.Л. Петрик, Ю.С. Манжос

# Калибровка чувствительности дескрипторного семантического контроля программного обеспечения информационно-управляющих систем

*Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ»*

Представлена процедура калибровки чувствительности дескрипторного семантического контроля программного обеспечения информационно-управляющих систем. Приведены качественные результаты калибровки в режиме статического и динамического анализов, показавшие, что применение дескрипторного семантического контроля обеспечивает достаточно точную оценку вероятности существования остаточных программных дефектов.
***Ключевые слова:*** независимая верификация, калибровка, дескрипторный семантический контроль, семантические инварианты, остаточные программные дефекты, статический анализ, динамический анализ.

## Введение

Надежность и безопасность современных информационно-управляющих систем (ИУС) критического применения существенно зависят от вероятности наличия остаточных дефектов (ОД) программного обеспечения (ПО). Основным механизмом снижения рисков, связанных с ОД ПО, является проведение независимой верификации (НВ) при сертификационных испытаниях с использованием диверсных методов на базе статического анализа (СА) исходного ПО. Количественная оценка уровня рисков, связанных с ОД ПО, возможна на основе калибровки методов путем инъекции программных дефектов с повторением цикла СА исходного кода. При этом определяют экспериментальные вероятности наличия дефектов, выявляемых диверсными методами.

## 1. Постановка задачи

Использование при сертификации классических методов верификации неэффективно ввиду их большой ресурсоемкости и корреляции с методами разработчиков. Достоверность НВ снижается ввиду неполноты контроля всех функциональных свойств, неполноты документирования ПО либо невозможности ввода всех программных характеристик в условиях ограниченных ресурсов сертификационных центров. НВ ПО ИУС, выполняемая сертификационными центрами, возможна посредством формального доказательства частичной корректности, основанного на применении дескрипторного семантического контроля (ДСК) [1].

В основу ДСК положено использование физической размерности (ФР) операндов (семантики) – программного инварианта, сохраняющего свои значения во всем диапазоне входных данных на протяжении времени работы программы. Нарушение семантики свидетельствует о наличии так называемых семантических дефектов. Применение целочисленного семантического отображения, которое взаимно-однозначно сопоставляет с каждой ФР операнда целое число – целочисленный семантический дескриптор (ЦСД), позволяет без разработки дополнительных версий функционального ПО, а лишь посредством контроля семантической корректности диагностировать вычислительные процессы (ВП) в реальном времени, упростить дистанционную модификацию и сопровождение ПО и, как

следствие, повысить надежность современных ИУС. В отличие от основной семантическая версия ПО дает возможность не только сформировать семантический результат, но и семантически верифицировать ПО на всех архитектурных уровнях [2].

В соответствии с дескрипторной моделью и методом НВ ПО, позволяющим повысить достоверность оценки качества и надежность ПО благодаря ДСК программных инвариантов – целочисленных семантических дескрипторов, разработана информационная технология НВ ПО в условиях ресурсных ограничений и неполноты проектной документации, которая внедрена в интегрированную систему поддержки экспертизы и НВ ПО систем критического применения, а также в систему комплексной динамической отработки ПО ИУС [3].

Информационная технология НВ обеспечивает решение следующих задач:

- повышение достоверности оценок характеристик ПО за счет реализации принципов технологического разнообразия (диверсности и независимости) на основе семантических, интервально-точностных и других инвариантов ПО;
- диверсифицированное измерение инвариантов ПО, при этом критерием для оценки измеренного инварианта является его ФР;
- оценку полноты тестового покрытия критического ПО при сертификации;
- прогнозирование вероятности ОД ПО путем экспериментальной калибровки чувствительности ДСК ПО ИУС, заключающейся в уточнении достоверности проведенной оценки методом инъекции известного количества семантических дефектов программного обеспечения (ДПО) в дескрипторную модель объекта экспертизы (ОЭ) с последующим ее анализом, что позволило откалибровать чувствительность ДСК на выявление ДПО для конкретного программного кода, уточнить достоверность проведенной оценки качества ПО.

## 2. Калибровка чувствительности дескрипторного семантического контроля ПО ИУС

ДСК позволяет выявлять следующие классы семантических ДПО:

1) использование неверных идентификаторов, типов операндов, операций в арифметических и логических выражениях;
2) семантические несоответствия формально-фактических параметров;
3) применение неверных адресов операндов;
4) использование неверных операций;
5) нарушение хода ВП, связанное с пропуском некоторых программных модулей или выполнением «лишних» программных модулей.

Классы и количество инъектированных дефектов для конкретного проекта ПО, определяемые на основании анализа использованных языковых конструкций и их возможных искажений, формируют профиль дефектов.

Во время калибровки выполняется искажение семантического контекста (СК) – множества семантических характеристик всех программных переменных. Для этого согласно профилю дефектов и статистическим характеристикам ПО (общего количества операций и уровня дефектов) формируется матрица инъекции. Далее реализуется инъекция ДПО в дескрипторную модель ОЭ и ее последующий анализ [4].

Инъекция дефектов осуществляется для каждого из программных выражений, которые связывают два операнда и инструкцию (операцию) в количестве, определяемом профилем ДПО, желаемым остаточным уровнем ДПО $P_{def}$, а также общим количеством инструкций, содержащихся в программном коде.

В результате СА в базе данных накапливается информация об обнаружен-

ных инъектированных ДПО. Цикл «статический анализ – калибровка» выполняется до исчерпания профиля инъектированных ДПО.

Прогнозируемое количество остаточных семантических ДПО определяется для каждого из программных модулей по формуле [5]

$$N_0 = \frac{n_s n_i}{n_{if}}, \quad (1)$$

где $N_0$ – прогнозированное количество семантических ОД ПО;

$n_s$ – количество выявленных реальных ОД;

$n_i$ – общее количество инъектированных ДПО;

$n_{if}$ – общее количество инъектированных ДПО, которые были выявлены.

Достоверность приведенной выше оценки определяется как

$$\eta = 1 - \frac{N_0}{N_{co}}, \quad (2)$$

где $N_{co}$ – подсчитанное количество использованных команд и операторов.

Анализ обнаруженных ДПО среди инъектированных с учетом специфики конкретного ПО позволяет найти практическую проверяющую способность ДСК $P$, которая определяется как отношение общего количества $n_{if}$ инъектированных выявленных ДПО к общему количеству инъектированных ДПО $n_i$

$$P = n_{if} / n_i, \quad (3)$$

где $P$ – практическая проверяющая способность ДСК;

$n_i$ – общее количество инъектированных ДПО;

$n_{if}$ – общее количество инъектированных ДПО, которые были выявлены.

## 3. Результаты калибровки чувствительности дескрипторного семантического контроля ПО ИУС

Все множество операций может быть условно разделено на аддитивные $A$ – сложение, вычитание, присваивание, сравнение, вызовы функций и процедур, и мультипликативные $M$ – умножение, деление, возведение в степень. Далее предполагается, что операции имеют два операнда, а вызовы функций и процедур рассматриваются как $n$-арные операции. Аддитивные операции не порождают новые ФР и используются в качестве контрольных точек при ДСК корректности ПО. Результаты мультипликативных операций имеют ФР, отличную от ФР операндов.

Результаты калибровки ДСК ПО в режиме статического и динамического анализов показаны в табл. 1-4, которые представляют собой ортогональную классификацию, основанную на характеристиках операндов и операций, функций, процедур.

В таблицах использованы следующие обозначения:

$P_S$ – проверяющая способность ДСК для выражений, содержащих только простые переменные;

$P_A$ – проверяющая способность ДС для выражений, использующих адресуемые данные (массивы и элементы, управляемые указателями);

$O_i$ – $i$-й операнд, $i=1,\ldots,n$, где $n$ – количество операндов;

$O_{if}$, $O_{ir}$ – фактическое и требуемое значение $i$-го операнда;

$D_f(O_i)$ – фактическое значение ЦСД $i$-го операнда операции;

$D_r(O_i)$ – требуемое значение ЦСД $i$-го операнда операции;

$A_f$, $A_r$ – фактическая и требуемая аддитивные операции;

$M_f$, $M_r$ – фактическая и требуемая мультипликативные операции;

$F_f$, $F_r$ – фактический и требуемый вызовы функций (передача множества параметров и возврат результата с определенными семантиками);

$P_f$, $P_r$ – фактический и требуемый вызовы процедур (передача множества параметров и возврат результата, содержащегося в параметрах, имеющих определенные семантики).

Инъектируются ДПО, связанные как с операндами, так и с операциями.

В табл. 1-2 рассмотрены ДПО, при которых в результате искажения аддитивная операция превращается в другую аддитивную ($A_f \neq A_r$) или мультипликативную ($A_r \Rightarrow M_f$); мультипликативная – в другую мультипликативную ($M_f \neq M_r$) или аддитивную ($M_r \Rightarrow A_f$). Если $A_f = A_r$, $M_f = M_r$, то искажения операции не произошло. Любое искажение операции присваивания распознается компилятором алгоритмического языка, поэтому возможный ДПО может быть связан только с характеристиками операндов.

Возможны случаи ДПО различной кратности. Однократный ДПО вызван искажением либо характеристики операнда, либо кода операции. Двукратные ДПО проявляются искажением кода операции и характеристики операнда.

На эффективность распознавания ДПО существенно влияют статистические характеристики ПО – операционный спектр (процентный состав операций) [6] и семантический спектр ПО (семантическое распределение данных по различным значениям ЦСД), а также достоверность выбранной системы единиц [7], зависящая от количества различных физических величин, имеющих совпадающие ФР. При искажении операций, приводящих к искажению операндов, возможно случайное совпадение ФР полученного фактического результата с требуемое ФР операнда. Поэтому в некоторых случаях доля обнаруженных ДПО среди инъектированных согласно (3) близка к 100%.

Таблица 1

Результаты калибровки ДСК ПО выражений, содержащих арифметические операции, присваивание и сравнение в режиме СА

<table>
<tr><td colspan="2" rowspan="4">Характеристики операций</td><td colspan="5">Характеристики операндов</td></tr>
<tr><td colspan="2">$D_f(O_1) \neq D_r(O_1)$</td><td colspan="3">$D_f(O_1)=D_r(O_1)$</td></tr>
<tr><td>$D_f(O_2)\neq D_r(O_2)$</td><td>$D_f(O_2)=D_r(O_2)$</td><td>$D_f(O_2)\neq D_r(O_2)$</td><td colspan="2">$D_f(O_2)=D_r(O_2)$</td></tr>
<tr><td></td><td></td><td></td><td>$O_{1f}=O_{1r}$, $O_{2f}=O_{2r}$</td><td>$O_{1f}\neq O_{1r}$ или $O_{2f}\neq O_{2r}$</td></tr>
<tr><td rowspan="6">Статический анализ</td><td>$A_f=A_r$</td><td>$P_S<1$, $P_A=0$</td><td colspan="2">$P_S=1$, $P_A=0$</td><td>ДПО отсутствуют</td><td>$P_S=0$, $P_A=0$</td></tr>
<tr><td>$M_f=A_r$</td><td rowspan="3"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="3"></td></tr>
<tr><td>$A_f=A_r$</td><td>$P_S=0$, $P_A=0$</td></tr>
<tr><td>$A_f=A_r$</td><td colspan="2">$P_S<1$, $P_A=0$</td><td colspan="2">$P_S=1$, $P_A=0$</td></tr>
<tr><td>$A_f=A_r$</td><td rowspan="2"></td><td colspan="2" rowspan="2">$P_S=1$, $P_A=0$</td><td>ДПО отсутствуют</td><td>$P_S=0$, $P_A=0$</td></tr>
<tr><td>$A_f = A_r$</td><td>$P_S=1$, $P_A=0$</td><td colspan="2">$P_S=1$, $P_A=0$</td></tr>
</table>

Таблица 2

Результаты калибровки ДСК ПО выражений, содержащих арифметические операции, присваивание и сравнение в режиме динамического анализа

<table>
<tr><td colspan="2" rowspan="3">Характе-ристики операций</td><td colspan="5">Характеристики операндов</td></tr>
<tr><td colspan="2">$D_f(O_1) \neq D_r(O_1)$</td><td colspan="3">$D_f(O_1) = D_r(O_1)$</td></tr>
<tr><td>$D_f(O_2) \neq D_r(O_2)$</td><td>$D_f(O_2) = D_r(O_2)$</td><td>$D_f(O_2) \neq D_r(O_2)$</td><td colspan="2">$D_f(O_2) = D_r(O_2)$</td></tr>
<tr><td rowspan="7">Динамический анализ</td><td>$A_f = A_r$</td><td rowspan="4">$P_S<1$, $P_A<10$</td><td colspan="2" rowspan="2">$P_S=1$, $P_A=1$</td><td>ДПО отсутствуют</td><td>$P_S=0$, $P_A=0$</td></tr>
<tr><td>$M_f = M_r$</td><td>$P_S=0$, $P_A=0$</td></tr>
<tr><td>$A_f \neq A_r$</td><td colspan="2">$P_S<1$, $P_A<1$</td><td colspan="2">$P_S=1$, $P_A=1$</td></tr>
<tr><td>$M_f \neq M_r$</td><td colspan="2" rowspan="2">$P_S=1$, $P_A=1$</td><td>ДПО отсутствуют</td><td>$P_S=0$, $P_A=0$</td></tr>
<tr><td>Прсва-ивание</td><td>$P_S=1$, $P_A=1$</td><td colspan="2">$P_S=1$, $P_A=1$</td></tr>
<tr><td colspan="2">$A_r \Rightarrow M_f$<br>$M_r \Rightarrow A_f$</td><td colspan="3">$P_S=1$, $P_A=1$</td></tr>
</table>

В табл. 3-4 для операций вызова функции *F* и процедур *P* рассмотрены ДПО, вызванные: искажением операндов – параметров функций или процедур, искажением имен функций ($F_f \neq F_r$) или процедур ($P_f \neq P_r$). Если $F_f = F_r$, $P_f = P_r$, то искажения имен функций или процедур не произошло.

Таблица 3

Результаты калибровки ДСК ПО выражений, содержащих вызовы функций и процедур в режиме СА

<table>
<tr><td colspan="4" rowspan="3">Характеристики операций</td><td colspan="3">Характеристики операндов</td></tr>
<tr><td>$\exists i \in 1..n$<br>$D_f(O_i) \neq D_r(O_i)$</td><td colspan="2">$\forall i \in 1..n\ D_f(O_i) = D_r(O_i)$</td></tr>
<tr><td>$\forall i \in 1..n$<br>$O_{fi} = O_{ri}$</td><td>$\forall i \in 1..n$<br>$O_{fi} \neq O_{ri}$</td></tr>
<tr><td rowspan="4">Статический анализ</td><td rowspan="3">функции</td><td rowspan="2">$DF_f = DF_r$</td><td>$F_f = F_r$</td><td>$P_S=1$, $P_A=0$</td><td>ДПО отсутствуют</td><td>$P_S=0$, $P_A=0$</td></tr>
<tr><td>$F_f \neq F_r$</td><td>$P_S<1$, $P_A=0$</td><td colspan="2" rowspan="2">$P_S<1$, $P_A=0$</td></tr>
<tr><td colspan="2">$DF_f \neq DF_r$</td><td>$P_S=1$, $P_A=0$</td></tr>
<tr><td>процедуры</td><td colspan="2">$P_f = P_r$</td><td rowspan="2"></td><td>ДПО отсутствуют</td><td>$P_S=0$, $P_A=0$</td></tr>
<tr><td colspan="2">$P_f \neq P_r$</td><td colspan="2">$P_S<1$, $P_A=0$</td></tr>
</table>

Таблица 4

Результаты калибровки ДСК ПО выражений, содержащих вызовы функций и процедур в режиме динамического анализа

<table>
<tr><td colspan="4">Характеристики операций</td><td colspan="3">Характеристики операндов</td></tr>
<tr><td colspan="4" rowspan="2"></td><td>$\exists i \in 1..n$<br>$D_f(O_i) \neq D_r(O_i)$</td><td colspan="2">$\forall i \in 1..n\ D_f(O_i) = D_r(O_i)$</td></tr>
<tr><td>$\forall i \in 1..n$<br>$O_{fi} = O_{ri}$</td><td>$\forall i \in 1..n$<br>$O_{fi} \neq O_{ri}$</td></tr>
<tr><td rowspan="4">Динамический анализ</td><td rowspan="3">Функции</td><td rowspan="2">$DF_f = DF_r$</td><td>$F_f = F_r$</td><td>$P_S$=1, $P_A$=1</td><td>ДПО отсутствуют</td><td>$P_S$=0, $P_A$=0</td></tr>
<tr><td>$F_f \neq F_r$</td><td>$P_S$<1, $P_A$=0</td><td colspan="2" rowspan="2">$P_S$<1, $P_A$<1</td></tr>
<tr><td colspan="2">$DF_f \neq DF_r$</td><td rowspan="3">$P_S$=1, $P_A$=1</td></tr>
<tr><td rowspan="2">Процедуры</td><td colspan="2">$P_f = P_r$</td><td>ДПО отсутствуют</td><td>$P_S$=0, $P_A$=0</td></tr>
<tr><td colspan="2">$P_f \neq P_r$</td><td colspan="3">$P_S$<1, $P_A$<1</td></tr>
</table>

Как видно из табл. 2, 4, ДСК в режиме динамического анализа позволяет обнаруживать ДПО для выражений, использующих адресуемые данные.

Результаты калибровки – количество инъектированных/обнаруженных дефектов и статистические характеристики проекта (спектры операций и данных, общее количество использованных операндов и операций) являются входными данными для процедуры формирования сводного отчета, главное назначение которой – обработка результатов, оценка характеристик качества ПО, формирование сводной оценки корректности ПО ИУС.

## Заключение

Метод дескрипторного семантического контроля, обеспечивающий контроль корректности ПО как в режиме СА, так и на этапе стендовой отработки или в реальном времени, имеет высокую диагностирующую способность. Достоверность результатов НВ с использованием ДСК, полученная в результате применения калибровки, составила 0,89. Результаты калибровки ДСК ПО в режиме статического и динамического анализов показали, что использование ДСК обеспечивает достаточно точную оценку вероятности существования остаточных программных дефектов.

## Список литературы

1. Петрик, В.Л. Метод дескрипторного контроля семантической корректности программного обеспечения [текст] / В.Л. Петрик // Системи управління, навігації та зв'язку: зб. наук. праць Центр. наук.-дослід. ін-ту навігації і управління. – 2007. – Вип.4. – С.140-143.

2. Петрик, В.Л. Целочисленное семантическое отображение [текст] / В.Л. Петрик // Радіоелектронні і комп'ютерні системи. – 2007. – №3(22). – С.73-81.

3. Петрик, В.Л. Інформаційна технологія верифікації програмного забезпечення інформаційно-управляючих систем на основі дескрипторної моделі: автореф. дис. … канд. техн. наук : 05.13.06 «Інформаційні технології» / В.Л. Петрик. –Х., 2009. – 20 с.

4. Калибровка чувствительности методов статического анализа, используемых для оценки качества и безопасности ПО ИУС АЭС [текст] / Б.М. Конорев, Т.А. Клименко, Ю.С. Манжос, В.Л. Петрик // Інтегровані комп'ютерні технології в машинобудуванні – ІКТМ 2004: Міжнар. наук.-техн. конф.: тези доп. – Х., 2004. – С. 400.

5. Майерс, Г. Надежность программного обеспечения / Г. Майерс [текст]: пер. с англ. – М.: Мир, 1980. – 360 с.

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

7. Конорев, Б.М. Обоснование выбора системы единиц физических величин для независимой верификации при сертификации программного обеспечения [текст] / Б.М. Конорев, В.Л. Петрик // Открытые информационные и компьютерные интегрированные технологии: сб. науч. тр. Нац. аэрокосм. ун-та им. Н.Е. Жуковского «ХАИ». – Вып. 33. – Х., 2006. – С.116-120.

**Рецензент:** д-р техн. наук, проф., В.П. Божко, Харьковский национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

Поступила в редакцию 16.03.12

## Калібрування чутливості дескрипторного семантичного контролю програмного забезпечення інформаційно-управляючих систем

Описано процедуру калібрування чутливості дескрипторного семантичного контролю програмного забезпечення інформаційно-управляючих систем. Наведено якісні результати калібрування в режимі статичного та динамічного аналізу. Результати показали, що застосування дескрипторного семантичного контролю забезпечує досить точне оцінювання ймовірності існування залишкових програмних дефектів.

***Ключові слова:*** незалежна верифікація, калібрування, дескрипторний семантичний контроль, семантичні інваріанти, остаточні програмні дефекти, статичний аналіз, динамічний аналіз.

## Calibration of descriptor semantic independence verification checking ability for I&C system software

Procedure calibration of descriptor semantic independence verification checking ability for I&C system software was presented in this article. The independence verification based on the semantic software invariants presented as semantic descriptor forms. Semantic descriptor is a integral number produced from semantic vector with scalar multiplication on the special number – nuclear of imaging between the semantic space and integral number. Quality results show the probabilities for different kind of software defects founded in the statical and dynamical modes.

***Keywords:*** independence verification, calibration, descriptor semantic checking, semantic invariants, latent software defects, statical analysis, dynamical analysis.