УДК 681.3(075.8)

В.С. ХАРЧЕНКО[1], В.В. СКЛЯР[2], Ю.А. БЕЛЫЙ[3]

[1]*Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина*
[2]*Государственный НТЦ по ядерной и радиационной безопасности, Украина*
[3]*Научно-производственное предприятие «Радий», Украина*

МОДЕЛИ ДЕФЕКТОВ МНОГОВЕРСИОННЫХ СИСТЕМ С УЧЕТОМ РАЗНООБРАЗИЯ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В статье получены модели дефектов мультидиверсных систем, учитывающие разнообразие программного обеспечения и технических средств, Проанализированы особенности формирования множеств дефектов отдельных программно-аппаратных версий и систем на их основе, а также процессов обнаружения дефектов и их парирования при функционировании.

многоверсионная система, модель дефектов

1. Определение мультидиверсной системы. Постановка задачи

Парадигма многоверсионности применяется в аэрокосмической техники и на АЭС при построении высоконадежных автоматических и человеко-машинных бортовых и наземных компьютерных систем управления [1 – 3].

Одновременно для системы может быть применено несколько видов версионной избыточности, (например, аппаратная, программная, субъектная, проектная, функциональная, сигнальная) [4]. Такой подход может быть назван мультидиверсным (в отличие от более общего многоверсионного, который подразумевает наличие по крайней мере одного вида версионной избыточности) [2]. Мультидиверсность является развитием принципа защиты в глубину, что позволяет снизить вероятность проявления отказов по общей причине [5 – 7].

Мультидиверсной будем называть такую двухверсионную систему W, в которой версии v_1, v_2 получены с использованием нескольких видов версионной избыточности, таких что устранение одного из этих видов избыточности не делает версии тождественными.

Если обозначить версии, в которых используется два и более видов разнообразия как $v_1(r)$, $v_2(r)$, где r – число таких видов, то r-диверсная система будет быть представлена следующим выражением:

$$W = \{X, F, U, V, R, \theta, Z\}\ , \qquad (1)$$

где X, U – входные и выходные сигналы;

F – множество выполняемых функций;

V – множество (двухместное) версий v_1, v_2 с выходными сигналами U_1 U_2;

Z – функция обработки результатов выполнения версий (отображения U_1, U_2 в U);

R – множество видов используемой версионной избыточности, причем $v_j \in V$ определяются на множестве R с помощью отображения θ.

Проведем более детальный анализ дефектов программного обеспечения (ПО) и технических средств (ТС) в мультидиверсной системе (МДВС). Необходимость такого исследования обусловлено следующими двумя причинами:

1) это необходимо для того, чтобы получить модели, на основе которых можно будет рассчитать метрики диверсности для последующего их учета в моделях надежности [8];

2) в процессе исследования необходимо уточнить свойства систем рассматриваемого класса.

Целью данной статьи является разработка теоретико-множественных моделей дефектов МДВС, учитывающих дефекты ПО и ТС.

2. Модели дефектов программного обеспечения и технических средств

Версия (канал) (пусть это будет первая версия V_1) в мультидиверсной системе представляет собой объединение ПО и ТС, для которых характерны три множества дефектов проектирования ПО – $D1^{ПО}$, дефектов проектирования (и производства) ТС – $D1^{TC}$ и физических дефектов ТС, возникающих в процессе использования системы (версии) по назначению.

Дефекты проектирования ПО и ТС имеют место вследствие неидеальной разработки и тестирования этих средств и проявляются при определенных входных данных. Тогда множество дефектов версии V_1:

$$DV1 = D1^{ПО} \cup D1^{TC} \cup D1_{TC};$$
$$D1^{ПО} = \{d1_i^{ПО}\}_{i=1}^{n_{по}};\ D1^{TC} = \{d1_j^{TC}\}_{j=1}^{n_{тс}};\qquad (2)$$
$$D1_{TC} = \{d1_{TCk}\}_{k=1}^{n_{TC}}.$$

Для элементов, входящих во множество DV1, справедливо:

$$\forall d1_i \in DV1:\ \exists x_s \in x,\ U(d1_i, x_s) \neq U(\varnothing, x_s).$$

Другими словами, дефект проявляется в виде искажения выходного сигнала системы хотя бы на одном входном наборе.

Множество искажаемых в результате проявления дефектов выходных сигналов U^* образует совместно с множеством U выходной алфавит системы (рис. 1):

$$U^{\Sigma} = U \cup U^*, \text{ где } U^* = U^{ПО*} \cup U^{TC*} \cup U^*_{TC},$$

где $U^{ПО*}$, U^{TC*}, U^*_{TC} – множества выходных сигналов, искажаемых в результате дефектов из множеств $D1^{ПО}$, $D1^{TC}$, $D1_{TC}$.

Кроме того, будем полагать, что элементы множеств не обладают свойством внутренней компенсации, т.е. для любого из этих множеств справедливо выражение:

$$\bar{\exists}(d1_i,\ d1_j);\ d1_i \neq d1_j \&$$
$$\& \ \bar{\exists} X_S \in X: U(d1_i,\ d1_j,\ X_S) = U(\varnothing, \varnothing, X_S). \qquad (3)$$

Возможны следующие варианты соотношений при объединении множеств $D1^{ПО}$, $D1^{TC}$ и $D1_{TC}$ (рис. 2).

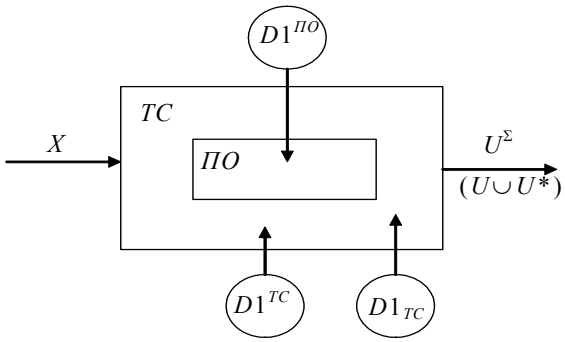

Рис. 1. Общая модель дефектов версии

1. Множества дефектов не пересекаются (рис. 2, а), т.е.:

$$D1^{ПО} \cap D1^{TC} = D1^{ПО} \cap D1_{TC} = D1^{TC} \cap D1_{TC} = \varnothing,$$
$$|\ DV1\ | = |\ D1^{ПО}\ | + |\ D1^{TC}\ | + |\ D1_{TC}\ |,$$

где $|\ X\ |$ – мощность множества X.

2. Пересекаются только два множества дефектов (рис. 2, б-г):

$$D1^{ПО} \cap D1^{TC} \neq \varnothing,\quad |\ D1^{ПО} \cup D1^{TC}\ | < |\ D1^{ПО}\ | + |\ D1^{TC}\ |;$$

$$D1^{ПО} \cap D1_{TC} \neq \varnothing,\quad |\ D1^{ПО} \cup D1_{TC}\ | < |\ D1^{ПО}\ | + |\ D1_{TC}\ |;$$

$$D1^{TC} \cap D1_{TC} \neq \varnothing,\quad |\ D1^{TC} \forall D1_{TC}\ | < |\ D1^{TC}\ | + |\ D1_{TC}\ |.$$

3. Пересекаются все три множества дефектов (рис. 2, д):

$$D1^{ПО} \cap D1^{TC} \neq \varnothing,\ D1^{ПО} \cap D1_{TC} \neq \varnothing;$$
$$D1^{TC} \cap D1_{TC} \neq \varnothing;$$
$$|\ D1^{ПО} \cup D1^{TC} \cup D1_{TC}\ | < |\ D1^{ПО}\ | + |\ D1^{TC}\ | + |\ D1_{TC}\ |.$$

Последнее из выражений может быть справедливо при попарном пересечении множеств дефектов, когда (рис. 2, е-з):

$$D1^{ПО} \cap D1^{TC} \neq \varnothing,\ D1^{ПО} \cap D1_{TC} \neq \varnothing,\ D1^{TC} \cap D1_{TC} = \varnothing$$

или

$$D1^{ПО} \cap D1_{TC} \neq \varnothing, D1^{TC} \cap D1_{TC} \neq \varnothing,\ D1^{ПО} \cap \cap D1^{TC} = \varnothing$$

или

$$D1^{ПО} \cap D1^{TC} \neq \varnothing, D1^{TC} \cap D1_{TC} \neq \varnothing, D1^{ПО} \cap D1_{TC} = \varnothing.$$

Необходимо отметить, что возможен еще один тип ситуаций, описываемых следующим образом (рис. 3).

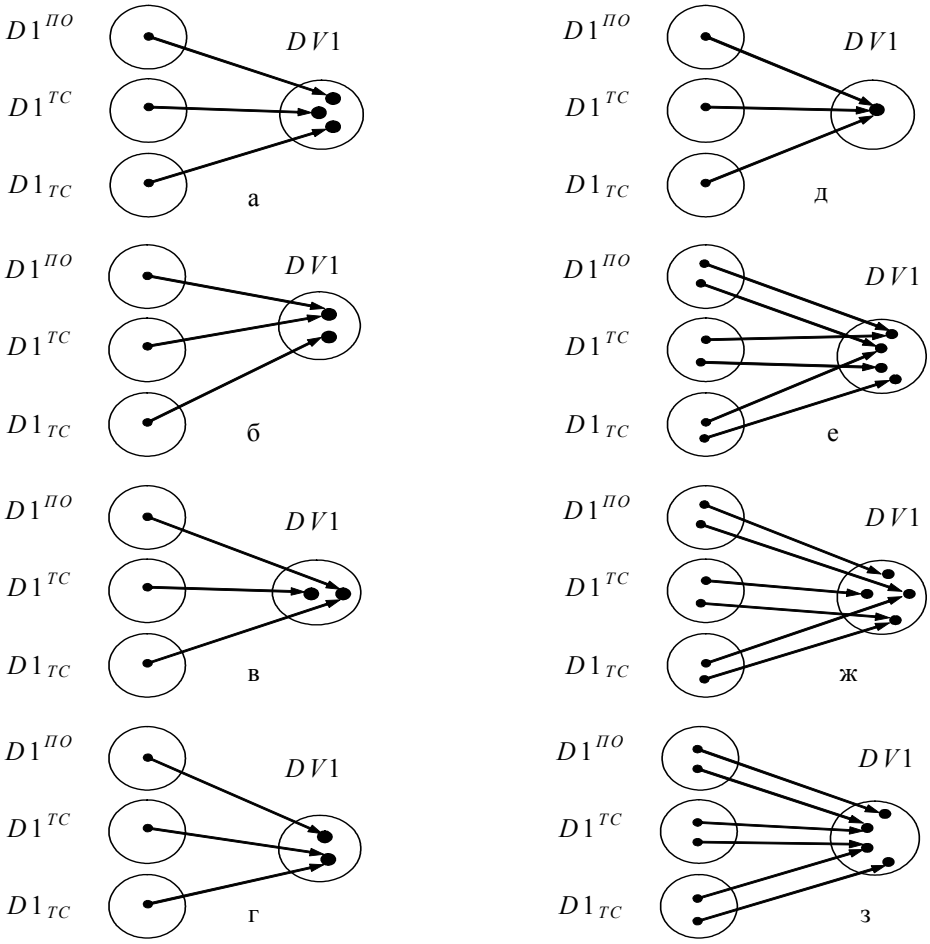

Рис. 2. Формирование множества дефектов версии в мультидиверсной системе

Если

$$\exists X_S \in X:\ [\exists(\ d1_i^{ПО}, d1_j^{ТС}):$$

$$U(\ d1_i^{ПО}, d1_j^{ТС}, X_S) = U(\varnothing,\varnothing,X_S)] \vee$$

$$\vee\ [\exists(\ d1_i^{ПО}, d1_{TCk}):\ U(\ d1_i^{ПО}, d1_{TCk}, X_S) =$$

$$= U(\varnothing,\varnothing,X_S)] \vee [\exists(\ d1_i^{ТС}, d1_{TCk}):$$

$$U(\ d1_i^{ТС}, d1_{TCk},\ X_S) = U(\varnothing,\varnothing,X_S)]$$

то имеет место эффект компенсации различных типов дефектов одной версии.

Такая ситуация иллюстрируется рис. 3, а-в. Рис. 3, г соответствует случаю, когда имеет место компенсация дефектов, принадлежащих всем трем множествам:

$$\exists(\ d1_i^{ПО},\ d1_j^{ТС}, d1_{TCk}):\ \forall(X_S) \in X,$$

$$U(\ d1_i^{ПО},\ d1_j^{ТС},\ d1_{TCk},\ X_S) = U(\varnothing,\varnothing,\varnothing,X_S).$$

Для эффекта парной компенсации справедливо:

$$|\ D1^{ПО} \times D1^{ТС} \cup D1^{ПО} \times D1_{ТС} \cup D1^{ТС} \times D1_{ТС}\ | <$$

$$< |\ D1^{ПО} \times D1^{ТС}\ | + |\ D1^{ПО} \times D1_{ТС}\ | + |\ D1^{ТС} \times D1_{ТС},,$$

где $\times$ – операция декартового произведения множеств.

Пары компенсируемых дефектов образуют множество $D1V_{\varnothing}$.

Таким образом, для множеств дефектов одной версии характерны свойства внутренней уникальности элементов одного множества по проявлению дефектов и возможность существования эффекта совпадения по последствиям и компенсации дефектов разных множеств.

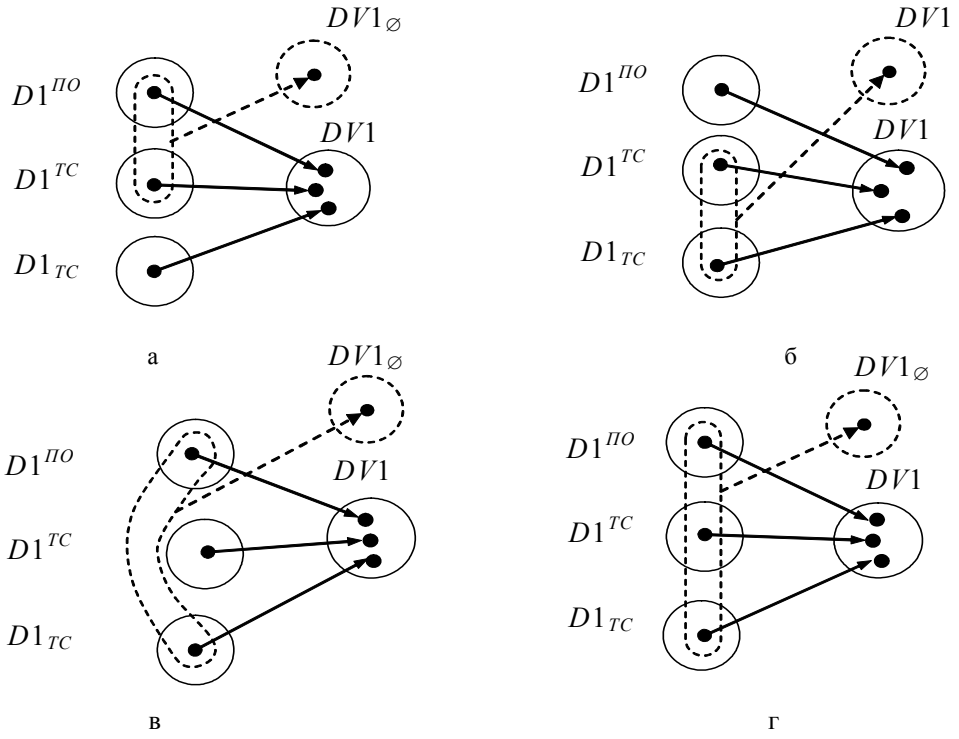

Рис. 3. Эффект компенсации дефектов

3. Последовательность формирования множества дефектов версии. Метрики сжатия и компенсации

Процедура формирования множества дефектов версии D1 включает следующие операции.

1. Определение множеств допустимых дефектов каждого типа $D1^{ПО}$, $D1^{TC}$, $D1_{TC}$.

Элементы каждого из множеств не должны иметь дефекты с одинаковыми последствиями на всех наборах входных сигналов $X_r \in X$.

2. Объединение элементов множеств $D1^{ПО}$, $D1^{TC}$, $D1_{TC}$ и получение множества $DV1$.

При объединении проводится сравнение последствий дефектов различных множеств и определяются дефекты, идентичные по последствиям:

$$d1_{\nu}^{ПО,TC} \in D1^{ПО,TC} = D1^{ПО} \cap D1^{TC},$$

если $D1^{ПО} \cap D1^{TC} \neq \varnothing$;

$$d1_{TC\mu}^{ПО} \in D1_{TC}^{ПО} = D1^{ПО} \cap D1_{TC},$$

если $1^{ПО} \cap D1_{TC} \neq \varnothing$;

$$d1_{TC\eta}^{TC} \in D1_{TC}^{TC} = D1^{TC} \cap D1_{TC},$$

если $D1^{TC} \cap D1_{TC} \neq \varnothing$.

Кроме того, могут быть учтены дефекты, принадлежащие всем трем исходным множествам, идентичные по последствиям $d1_{TC\sigma}^{ПО,TC} \in D1_{TC}^{ПО,TC}$.

3. Вычисляются коэффициенты (метрики) естественного сжатия множества дефектов версии DV1:

$$KS1 = (\left|D1^{ПО}\right| + \left|D1^{TC}\right| + \left|D1_{TC}\right| - \left|D1^{ПО,TC}\right| - \left|D1_{TC}^{ПО}\right| - \left|D1_{TC}^{TC}\right| - \left|D1_{TC}^{ПО,TC}\right|) / (\left|D1^{ПО}\right| + \left|D1^{TC}\right| + \left|D1_{TC}\right|). \quad (3)$$

Могут быть также вычислены аналогичные коэффициенты по каждому множеству:

$$KS1^{ПО} = \frac{\left|D1^{ПО} \setminus D1^{ПО,TC} \setminus D1_{TC}^{ПО}\right|}{\left|D1^{ПО}\right|};$$

$$KS1^{TC} = \frac{\left|D1^{TC} \setminus D1^{ПО,TC} \setminus D1_{TC}^{TC}\right|}{\left|D1^{TC}\right|};$$

$$KS1^{ПО} = \frac{\left|D1_{TC} \setminus D1_{TC}^{ПО} \setminus D1_{TC}^{TC}\right|}{\left|D1_{TC}\right|}.$$

4. Проводится анализ элементов множеств:

$D1_{X}^{ПО,TC} = D1^{ПО} \times D1^{TC}$, $D1_{TCX}^{ПО} = D1^{ПО} \times D1_{TC}$;

$D1_{TCX}^{TC} = D1^{TC} \times D1_{TC;}$

$D1_{TCX}^{ПО,TC} = D1^{ПО} \times D1^{TC} \times D1_{TC,}$ с точки зрения эффекта компенсации последствий.

Формируются множества компенсируемых дефектов:

$\mathrm{DV1}_{\varnothing}^{\mathrm{ПО,ТС}} \subset \mathrm{D1}_{X}^{\mathrm{ПО,ТС}}$; $\mathrm{DV1}_{TC\varnothing}^{\mathrm{ПО}} \subset \mathrm{D1}_{TCX}^{\mathrm{ПО}}$;

$\mathrm{DV1}_{TC\varnothing}^{\mathrm{ТС}} \subset \mathrm{D1}_{TCX}^{\mathrm{ТС}}$; $\mathrm{DV1}_{TC\varnothing}^{\mathrm{ПО,ТС}} \subset \mathrm{D1}_{TCX}^{\mathrm{ПО,ТС}}$.

Исходя из этого, определяется множество компенсируемых дефектов версии в целом:

$$\mathrm{DV1}_{\varnothing} = \mathrm{DV1}_{\varnothing}^{\mathrm{ПО,ТС}} \cup \mathrm{DV1}_{\varnothing}^{\mathrm{ПО}} \cup \mathrm{DV1}_{TC\varnothing}^{\mathrm{ТС}} \cup \mathrm{DV1}_{TC\varnothing}^{\mathrm{ПО,ТС}}.$$

При анализе эффектов сжатия и компенсации рассматриваются варианты ситуаций по выходным сигналам, приведенные в табл. 1.

Таблица 1

Варианты ситуаций с дефектами по выходным сигналам

$d_i^{ПО}$	$d_j^{ТС}$	d_{TCk}	Варианты выходных сигналов, U
∅	∅	∅	∅
∅	∅	1	$U(d_{TCk})$
∅	1	∅	$U(d_j^{ТС})$
∅	1	1	$U(d_j^{ТС})$ $U(\mathrm{d}_{TCk})$ $U(d_j^{ТС}, d_{TCk})$
1	∅	∅	$U(d_i^{ПО})$
1	∅	1	$U(d_i^{ПО})$ $U(d_{TCk})$ $U(d_i^{ПО}, d_{TCk})$
1	1	∅	$U(d_i^{ПО})$ $U(d_j^{ТС})$ $U(d_i^{ПО}, d_j^{ТС})$
1	1	1	$U(d_i^{ПО}), U(d_j^{ТС}), U(\mathrm{d}_{TCk})$ $U(d_i^{ПО}, d_j^{ТС}), U(d_i^{ПО}, d_{TCk})$, $U(d_j^{ТС}, d_{TCk})$, $U(d_i^{ПО}, d_j^{ТС}, d_{TCk})$

Модель дефектов версии представляется в виде пары множеств $DV1$ и $DV1_{\varnothing}$.

5. Вычисляются коэффициенты (метрики) компенсации дефектов для версии в целом:

$$KK1 = \frac{\left|DV1_{\varnothing}\right|}{\left|D1_{X}^{ПО,ТС}\right| + \left|D1_{TCX}^{ПО}\right| + \left|D1_{TCX}^{ТС}\right| + \left|D1_{TCX}^{ПО,ТС}\right|} \quad (4)$$

и пар множеств дефектов:

$$KK1^{ПО,ТС} = \frac{\left|DV1_{\varnothing}^{ПО,ТС}\right|}{\left|DV1_{X}^{ПО,ТС}\right|};$$

$$KK1_{TC}^{ПО} = \frac{\left|DV1_{TC\varnothing}^{ПО}\right|}{\left|DV1_{TCX}^{ПО}\right|};$$

$$KK1_{TC}^{ТС} = \frac{\left|DV1_{TC\varnothing}^{ТС}\right|}{\left|DV1_{TCX}^{ТС}\right|}.$$

4. Модель дефектов мультидиверсной системы

Для МДВС $V1\mathrm{ТС} \neq V2\mathrm{ТС}$ и $V1\mathrm{ПО} \neq V2\mathrm{ПО}$. Тогда, в общем случае имеем (рис. 4):

$$\begin{cases} D1^{ПО} \cap D2^{ПО} \neq \varnothing; \\ D1^{ТС} \cap D2^{ТС} \neq \varnothing; \\ D1_{TC} \cap D2_{TC} \neq \varnothing. \end{cases} \quad (5)$$

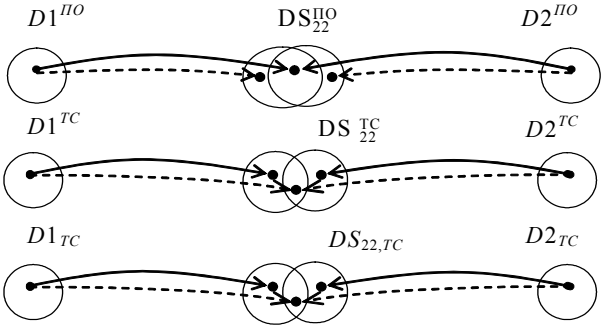

Рис. 4. Объединение дефектов мультидиверсной системы

Примером такой системы является мультидиверсная система аварийной защиты реактора, в которой используются двухверсионные ТС и двухверсионное ПО [3].

Множества дефектов ТС и ПО такой системы имеют вид:

$DS_{22}^{ПО} = D1^{ПО} \cup D2^{ПО}$; $DS_{22}^{ПО} = D1^{ТС} \cup D2^{ТС}$;

$DS_{22}^{ПО} = D1_{TC} \cup D2_{TC}$,

а общее множество

$DS_{22} = DS_{22}^{ПО} \cup DS_{22}^{ТС} \cup DS_{22TC}$.

Нижние индексы для множеств в последних выражениях, как и ранее, указывают на число версий и число видов версионной избыточности (ПО и ТС).

Последним выражениям соответствует графическая интерпретация (рис. 5), т.е. с учетом аспекта различимости дефектов получим

$$DS_{22}=(D1^{ПО}_{отн} \cup D1^{ТС}_{отн} \cup D1_{ТСотн}) \cup$$
$$\cup (D2^{ПО}_{отн} \cup D2^{ТС}_{отн} \cup D2_{ТСотн}) \cup (D12^{ПО}_{р} \cup D12^{ТС}_{р} \cup \quad (6)$$
$$\cup D2_{ТСр}) \cup (D12^{ПО}_{н} \cup D12^{ТС}_{н} \cup D2_{ТСн}).$$

В выражении (6) в круглых скобках сгруппированы множества однотипных дефектов: относительных ($Di_{отн}$) и абсолютных различимых ($D12_р$) и неразличимых ($D12_н$).

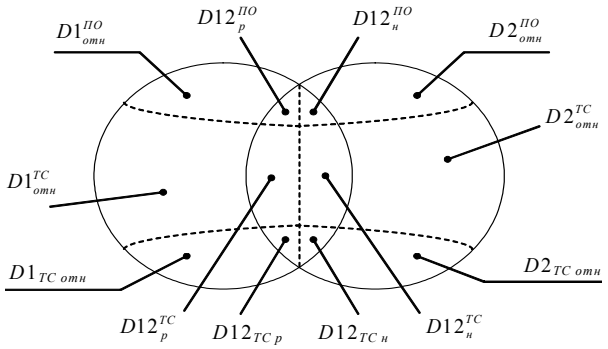

Рис. 5. Графическая интерпретация множества дефектов мультидиверсной системы

Выводы

В статье впервые получены модели дефектов мультидиверсных систем, отличающиеся от известных тем, что они учитывают разнообразие программного обеспечения и технических средств, особенности формирования множеств дефектов отдельных программно-аппаратных версий и систем, а также процессов их обнаружения и парирования при функционировании. Данный результат позволяет выполнять более точную оценку надежности мультидиверсных систем благодаря учету различных вариантов соотношения множеств дефектов и эффектов сжатия и компенсации.

Проведенный анализ проектов ИУС показал, что:

– доли дефектов трех типов (множества $D1^{ПО}$, $D1^{ТС}$, $D1_{ТС}$) колеблются для разных проектов в пределах 40-50%, 2-4%, 50-54% соответственно (сумма средних значений равна 100%);

– коэффициенты сжатия (KS1) и компенсации дефектов (KK) могут изменяться в пределах 0,05–0,1 и 0,04–0,06 соответственно.

Эти коэффициенты могут учитываться в вероятностных моделях мультидиверсных систем для выбора вариантов версионной избыточности.

Литература

1. Avizienis A., Laprie J., Randell B. Fundamental Concepts of Dependability. Research Report n 01145, LAAS-CNRS, 2001. – 25 p.

2. Харченко В.С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. – ХВУ, 1996. – 506 с.

3. Lyu M.R. Handbook of Software Reliability Engineering. – McGraw-Hill Company, 1996. – 805 p.

4. Preckshot G. Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems. NUREG/CR-6303. – Livermore, USA: Lawrence Livermore National Laboratory, 1994. – 35 p.

5. Sklyar V., Kharchenko V. A Method of Multiversion Technologies Choice on Development of Fault-Tolerant Software Systems // Proceeding of Workshop on Methods, Models and Tools for Fault Tolerance. – Oxford, UK, 2007. – P. 148-157.

6. Бахмач Е.С., Сиора А.А., Скляр В.В., Токарев В.И., Харченко В.С. Обеспечение и оценка безопасности информационных и управляющих систем АЭС на базе ПЛИС // Радіоелектронні і комп'ютерні системи. – 2007. – №. 7 (26). – С. 75-82.

7. Скляр В.В., Головир В.А. Задача оптимального выбора многоверсионных технологий // Радіоелектронні і комп'ютерні системи. – 2007. – № 7 (26).– С. 62-67.

8. Скляр В.В. Анализ метрик многоверсионности программного обеспечения // Электронное моделирование. – 2004. – Т. 26, № 4. – С. 95-104.

Поступила в редакцию 22.01.2008

Рецензент: д-р техн. наук, проф. Е.Ф. Кривуля, Харьковский национальный университет радиоэлектроники, Харьков.