УДК 004.415 : 004.412

**В.В. СКЛЯР[1], В.А. ГОЛОВИР[2]**

[1]*Государственный научно-технический центр по ядерной и радиационной безопасности, Украина*
[2]*ЗАО «Радий», Украина*

# ЗАДАЧА ОПТИМАЛЬНОГО ВЫБОРА МНОГОВЕРСИОННЫХ ТЕХНОЛОГИЙ РАЗРАБОТКИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Получена графовая модель жизненного цикла для многоверсионных информационно-управляющих систем. Формализована задача выбора многоверсионных технологий разработки информационно-управляющих систем. Такая задача может иметь четыре варианта постановки, которые имеют вид либо задач поиска кратчайшего/максимального пути в ориентированном графе, либо задач динамического программирования. Получены решения для четырех видов задачи оптимального выбора.

**задача оптимального выбора, многоверсионная технология**

## Постановка задачи и обзор публикаций

Применение многоверсионных технологий (МВТ) является действенным способом защиты информационно-управляющих систем (ИУС) от дефектов проектирования [1 - 3].

Базовым решением для внедрения МВТ является выбор различных программно-аппаратных платформ, на основе которых реализуются неидентичные версии ИУС [4]. Кроме того, на базе программно-аппаратного разнообразия могут быть реализованы следующие виды разнообразия [5]:

– субъектное разнообразие – достигается за счет привлечения различных исполнителей работ;

– проектное разнообразие – достигается за счет применения различных методов (подходов) проектирования аппаратных или программных средств;

– функциональное разнообразие – достигается за счет реализации различными версиями различной функциональности (различных физических функций или альтернативных алгоритмов);

– сигнальное разнообразие – достигается за счет использования различных входных параметров (различных источников данных) определяющих функционирование системы.

Высокая стоимость реализации МВТ выдвигает задачу оптимизации вложения ресурсов для получения максимально возможного эффекта по снижению дефектов, внесенных при разработке ИУС.

Особенности оценки стоимости применения МВТ изложены в работах [4, 6]. Для оценки эффекта применения МВТ целесообразно применять метрики диверсности [7 - 9], которые, с одной стороны, позволяют оценить различия между версиями ИУС, а с другой стороны, позволяют определить коэффициент снижения количества дефектов многоверсионной ИУС по сравнению с одноверсионной ИУС.

Задача формализации модели жизненного цикла многоверсионных ИУС решалась, например, в работах [4, 6, 10]. Однако, в известной литературе отсутствует решение задачи оптимального выбора МВТ.

**Целью статьи является** формализация и решение в общем виде задачи оптимального выбора МВТ разработки ИУС.

## 1. Графовая модель жизненного цикла многоверсионной ИУС

Жизненный цикл (ЖЦ) ИУС представляет собой последовательность $N$ этапов. На каждом $i$-м этапе ЖЦ многоверсионной ИУС возможно применение $M_i$ способов внесения версионной избыточности. Выбор многоверсионной технологии разработки

ИУС заключается в последовательном выборе на каждом *i*-м этапе ЖЦ *j*-го способа внесения версионной избыточности (СВВИ) ИУС. Анализ технологий разработки ИУС показывает, что в общем случае выбор на каждом *i*-м этапе ЖЦ *j*-го СВВИ не влияет на выбор на (*i* + 1)-м этапе [9]. Однако, это допущение не носит принципиального характера и не влияет на дальнейшее решение задачи выбора. Кроме того, на каждом *i*-м этапе ЖЦ может быть принято решение о выборе одноверсионной технологии. Такое решение также является независимым от предыдущих и последующих этапов ЖЦ. Каждый *j*-й СВВИ на каждом *i*-м этапе ЖЦ характеризуется двумя показателями: метрикой (степенью) диверсности $d_{ij}$ и стоимостью применения соответствующего СВВИ $c_{ij}$ (приращением стоимости по сравнению с одноверсионным вариантом *i*-го этапа ЖЦ).

Таким образом, возможное поле решений по выбору МВТ разработки ИУС описывается двумя матрицами: матрицей значений метрик диверсности $D = \| d_{ij} \|$ и матрицей значений стоимости $C = \| c_{ij} \|$, $i = 1,...,N$; $j = 1,...,M_i$. Отметим, что количество элементов матриц $M_i$ в *i*-м столбце в общем случае неодинаково и определяется количеством СВВИ для *i*-го этапа ЖЦ. С учетом возможности выбора на каждом *i*-м этапе ЖЦ одноверсионной технологии реализации ИУС, матрицы *D* и *C* могут быть дополнены нулевыми строками, содержащими *N* элементов: $D_0 = \| 0,...,0 \|$ и $C_0 = \| 0,...,0 \|$.

Таким образом, ЖЦ многоверсионной ИУС может быть представлен *N*-уровневым графом $G = \langle V,U \rangle$, где $V = \{v_{ij}\}$ – множество вершин графа, $U = \{(v_{i1j1}, v_{i2j2})\}$ – множество ребер графа, каждое ребро определяется парой соединяемых вершин. Добавив начальную вершину $V_S$ и вершину $V_F$, получим граф, имеющий вид сети (рис. 1).

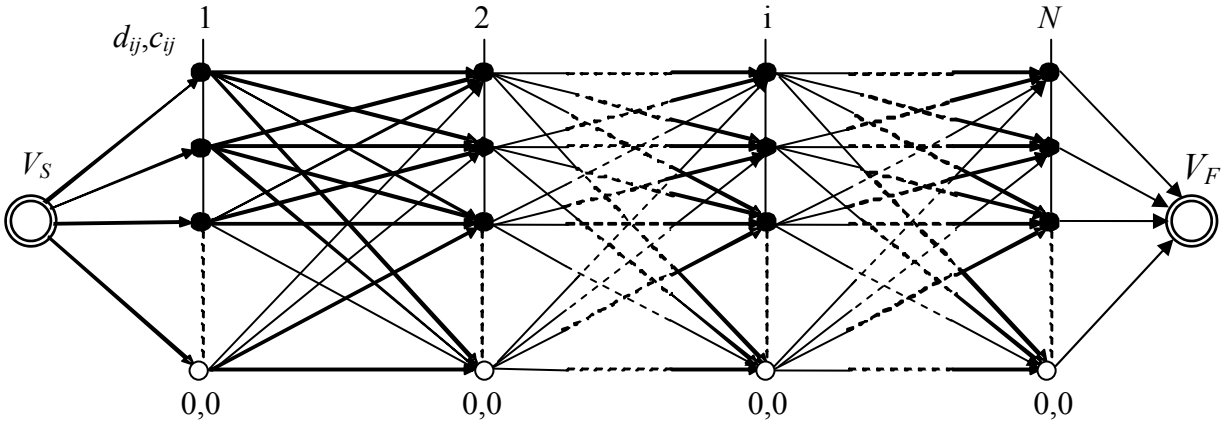


Рис. 1. Графовая модель жизненного цикла многоверсионной ИУС

Проанализируем свойства графа *G*, представленного на рис. 1.

1. Граф *G* является ориентированным (все ребра имеют направление), конечным (множество вершин и множество ребер являются конечными), связным (две любые вершины графа соединяются между собой одним или несколькими ребрами), простым (две любые вершины графа соединяются не более чем одним ребром).

2. Граф *G* является сетью, которая имеет вход $V_S$ и выход $V_F$.

3. Между входом и выходом графа *G* имеются *N* уровней. Ребра графа имеют направления от *i*-го к (*i* + 1)-му уровню, причем длина любого пути между двумя любыми соседними уровнями составляет одно ребро. Соответственно длина любого пути между входом и выходом графа *G* составляет (*N* + 1) ребро.

4. Количество вершин графа *G* для каждого из *N* уровней в общем случае является разным: $M_1 \neq M_2 \neq ... \neq M_i \neq ... \neq M_N$.

5. Каждая из вершин $v_{ij}$ $i$-го уровня графа $G$ связана ребром с каждой из вершин $v_{(i+1)k}$ $(i + 1)$-го уровня: $\forall\ v_{ij} : (v_{ij}, v_{(i+1)k})$. Это относится также и к «нулевым» вершинам $v_{i0}$, соответсвующим реализации одноверсионной технологии на $i$-м этапе ЖЦ.

6. Каждая из вершин $v_{ij}$ графа $G$ соответствует $j$-му СВВИ для $i$-го этапа ЖЦ. Каждой из вершин $v_{ij}$ приписывается значение $d_{ij}$ метрики диверсности, соответствующей данному СВВИ, а также значение $c_{ij}$ стоимости применения соответствующего СВВИ.

7. Матрицы значений метрик диверсности $D = \| d_{ij} \|$ и стоимости $C = \| c_{ij} \|$, $i = 1,...,N$; $j = 1,...,M_i$. имеют общую форму и в общем случае не являются прямоугольными.

8. Вершиы графа $G$ на каждом $i$-м уровне дополняются одной «нулевой» вершиной $v_{i0}$, соответсвующим реализации одноверсионной технологии на $i$-м этапе ЖЦ. Для этих вершин $d_{iM_{i+1}} = 0$, $c_{iM_{i+1}} = 0$. Таким образом, матрицы метрик диверсности $D$ и стоимости $C$ дополняются строками из $N$ нулевых элементов и принимают вид:

$$D' = \begin{Vmatrix} d_{11} & d_{21} & ... & d_{i1} & ... & d_{N1} \\ d_{12} & d_{22} & ... & d_{i2} & ... & d_{N2} \\ ... & ... & ... & ... & ... & ... \\ d_{1j} & d_{2j} & ... & d_{ij} & ... & d_{Nj} \\ ... & ... & ... & ... & ... & ... \\ d_{1M_1} & ... & ... & ... & ... & ... \\ - & ... & ... & d_{iM_i} & ... & ... \\ - & d_{2M_2} & ... & - & ... & d_{NM_N} \\ 0 & 0 & ... & 0 & ... & 0 \end{Vmatrix};$$

$$C' = \begin{Vmatrix} c_{11} & c_{21} & ... & c_{i1} & ... & c_{N1} \\ c_{12} & c_{22} & ... & c_{i2} & ... & c_{N2} \\ ... & ... & ... & ... & ... & ... \\ c_{1j} & c_{2j} & ... & c_{ij} & ... & c_{Nj} \\ ... & ... & ... & ... & ... & ... \\ c_{1M_1} & ... & ... & ... & ... & ... \\ - & ... & ... & c_{iM_i} & ... & ... \\ - & c_{2M_2} & ... & - & ... & c_{NM_N} \\ 0 & 0 & ... & 0 & ... & 0 \end{Vmatrix}.$$

Многоверсионной технологией разработки ИУС будем называть путь $MVT = \{V_S, v_{1j}, v_{2j},..., v_{ij}, v_{Nj}, V_F\}$, содержащий хотя бы одну вершину $v_{ij}$, отличную от «нулевой» $v_{i0}$. МВТ характеризуется суммарной метрикой диверсности $D = \sum_{i=1}^{N} d_{ij}$ и суммарной стоимостью (дополнительной по отношению к одноверсионной технологии) $C = \sum_{i=1}^{N} c_{ij}$.

Одноверсионная технология разработки ИУС соответствует пути $OVT = \{V_S, v_{10}, v_{20},..., v_{i0}, v_{N0}, V_F\}$, включающей только «нулевые» вершины $v_{i0}$. Соответсвенно, для одноверсионной технологии $D = 0$, $C = 0$.

## 2. Постановка и решение задачи оптимального выбора многоверсионных технологий разработки ИУС

Постановка задачи выбора МВТ разработки ИУС может иметь следующие четыре варианта:

1) найти $C_{\min}$ при реализации любой многоверсионной технологии $D \neq 0$;

2) найти $D_{\max}$ без учета ограничений по стоимости;

3) найти $C \to \min$ при $D \geq D_{заданное}$;

4) найти $D \to \max$ при $C \leq C_{заданное}$.

Первая задача является задачей поиска кратчайшего пути, а вторая – задачей поиска максимального пути [11,12]. Учитывая упрощенный вид сформулированных задач, целесообразно решать их не стандартными формализованными методами (такими, как метод Минти, метод потенциалов и т.п.) [13,14], а при помощи упрощенных эвристических процедур. Третья и четвертая задачи являются задачами динамического программирования, поскольку представление исходных данных в матричной форме подразумевает аддитивную целевую функцию и аддитивные ограничения [11].

***Задача 1*** нахождения $C_{\min}$ при реализации любой многоверсионной технологии $D \neq 0$ является задачей поиска кратчайшего пути для вершин графа $G$, помеченных значениями $c_{ij}$.

В общем случае кратчайшим будет путь через вершины $v_{i0}$, для которых $c_{i0} = 0$. Однако, при этом не выполняется условие $D \neq 0$, поскольку такая технология является одноверсионной. Поэтому для условия $D \neq 0$ кратчайшим будет путь, содержащий одну вершину $v_{ij}(c_{ij\,\min})$, а все остальные вершины $c_{i0} = 0$.

Решение задачи включает следующую последовательность действий:

1. Выбор $c_{ij} = c_{ij\,\min}$.

2. Если существует несколько вершин, для которых $c_{ij} = c_{ij\,\min}$, то следует выбрать ту вершину, для которой $d_{ij} = d_{ij\,\max}$.

Решением задачи является путь $MVT(C_{\min}) = \{V_S, v_{i0},..., v_{ij}(c_{ij\,\min}),\ldots, v_{i0}, V_F\}$. Для пути $MVT(C_{\min})$ имеем значение метрики диверсности $D = d[v_{ij}(c_{ij\,\min})]$ и значение стоимости $C = c_{ij\,\min}$.

***Задача 2*** нахождения $D_{\max}$ без учета ограничений по стоимости является задачей поиска максимального пути для вершин графа $G$, помеченных значениями $d_{ij}$.

Максимальным будет путь через вершины $v_{ij}(d_{i\,\max})$, для которых значения $d_{ij}$ являются максимальными для каждого $i$-го этапа ЖЦ.

Решение задачи включает следующую последовательность действий:

1. Выбор $d_{i\,\max}$.для каждого $i$-го этапа ЖЦ.

2. Если существует несколько вершин, для которых $d_{ij} = d_{i\,\max}$,то следует выбрать ту вершину, для которой $c_{ij} = c_{ij\,\min}$.

Решением задачи является путь $MVT(D_{\max}) = \{V_S, v_{1j}(d_{1\,\max}), v_{2j}(d_{2\,\max}),..., v_{ij}(d_{i\,\max}),\ldots, v_{Nj}(d_{N\,\max}), V_F\}$. Для пути $MVT(D_{\max})$ имеем значение метрики диверсности $D=\sum_{i=1}^{N} d_{i\,\max}$ и значение стоимости $C=\sum_{i=1}^{N} c\left[v_{ij}(d_{i\,\max})\right]$.

***Задача 3*** нахождения минимальной стоимости при заданном уровне диверсности ($C \to \min$ при $D \geq D_{заданное}$) является задачею динамического программирования.

Целевой функцией является $f(C)=\sum_{i=1}^{N} c_{ij} \cdot \frac{1}{d_{ij}} \to \min$ при ограничениях $\sum_{i=1}^{N} d_{ij} \geq D_{заданное}$.

Решение такой задачи включает следующую последовательность действий:

1. Присвоение суммарной метрике диверсности значения $D = 0$ и счетчику значения $k = 0$.

2. Построение матрицы $C^{(N-k)}/D^{(N-k)}=\left\|\frac{c_{ij}}{d_{ij}}\right\|$.

3. Выбор минимального элемента матрицы $\frac{c_{ij}}{d_{ij}}=\min$.

4. Если существует несколько элементов матрицы с одинаковым минимальным значением, то следует выбрать ту вершину, для которой $d_{ij} = d_{ij\,\max}$.

5. Присвоение суммарной метрике диверсности значения $D = D + d\left[v_{ij}\left(\frac{c_{ij}}{d_{ij}}=\min\right)\right]$ и счетчику значения $k = k + 1$. Включение вершины $v_{ij}\left(\frac{c_{ij}}{d_{ij}}=\min\right)$ в состав искомой многоверсионной технологии.

6. Проверка условия $D \geq D_{заданное}$.

7. Если условие, указанное в действии 6, выполняется, то выполнение алгоритма заканчивается, а уже выбранные вершины пути, соответствующего многоверсионной технологии, дополняются «нулевыми» вершинами $v_{i0}$.

8. Если условие, указанное в действии 6, не выполняется, то из матрицы $D^{(N-k)}/C^{(N-k)}$ удаляется столбец, содержащий элемент матрицы, выбранный на шаге 3. После этого снова выполняются шаги 3 - 8.

Решением задачи является путь $MVT(C \to \min) = \{V_S, v_{1j}\left(\frac{c_{1j}}{d_{1j}}=\min\right), v_{2j}\left(\frac{c_{2j}}{d_{2j}}=\min\right),$ $..., v_{ij}\left(\frac{c_{ij}}{d_{ij}}=\min\right),\ldots, v_{Nj}\left(\frac{c_{Nj}}{d_{Nj}}=\min\right), \mathrm{V_F}\}$. Для пути

$MVT(C \to \min)$ имеем значение метрики диверсности $D = \sum_{i=1}^{N} d\left[ v_{ij}\left( \frac{c_{ij}}{d_{ij}} = \min \right) \right]$ и значение стоимости $C = \sum_{i=1}^{N} c\left[ v_{ij}\left( \frac{c_{ij}}{d_{ij}} = \min \right) \right]$.

***Задача 4*** нахождения максимальной диверсности при заданном уровне стоимости ($D \to \max$ при $C \le C_{заданное}$) является задачею динамического программирования.

Целевой функцией является $f(D) = \sum_{i=1}^{N} d_{ij} \cdot \frac{1}{c_{ij}} \to \max$ при ограничениях $\sum_{i=1}^{N} c_{ij} \le C_{заданное}$.

Решение такой задачи включает следующую последовательность действий:

1. Присвоение суммарной стоимости значения $D = 0$ и счетчику значения $k = 0$.

2. Построение матрицы $C^{(N-k)} / D^{(N-k)} = \left\| \frac{d_{ij}}{c_{ij}} \right\|$.

3. Выбор максимального элемента матрицы $\frac{d_{ij}}{c_{ij}} = \max$.

4. Если существует несколько элементов матрицы с одинаковым максимальным значением, то следует выбрать ту вершину, для которой $c_{ij} = c_{ij\,\min}$.

5. Присвоение суммарной стоимости значения $C = C + c\left[ v_{ij}\left( \frac{d_{ij}}{c_{ij}} = \max \right) \right]$ и счетчику значения $k = k + 1$. Включение вершины $v_{ij}\left( \frac{d_{ij}}{c_{ij}} = \max \right)$ в состав искомой многоверсионной технологии.

6. Проверка условия $C \le C_{заданное}$.

7. Если условие, указанное в действии 6, не выполняется, то выполнение алгоритма заканчивается, а уже выбранные вершины пути, соответствующего многоверсионной технологии, дополняются «нулевыми» вершинами $v_{i0}$.

8. Если условие, указанное в действии 6, выполняется, то из матрицы $D^{(N-k)}/C^{(N-k)}$ удаляется столбец, содержащий элемент матрицы, выбранный на шаге 3.

После этого снова выполняются шаги 3 – 8.

Решением задачи является путь $MVT(D \to \max) = \{V_S, \quad v_{1j}\left( \frac{d_{1j}}{c_{1j}} = \max \right), \quad v_{2j}\left( \frac{d_{2j}}{c_{2j}} = \max \right), \ldots, v_{ij}\left( \frac{d_{ij}}{c_{ij}} = \max \right), \ldots, \quad v_{Nj}\left( \frac{d_{Nj}}{c_{Nj}} = \max \right), \quad V_F\}$. Для пути $MVT(D \to \max)$ имеем значение метрики диверсности $D = \sum_{i=1}^{N} d\left[ v_{ij}\left( \frac{d_{ij}}{c_{ij}} = \max \right) \right]$ и значение стоимости $C = \sum_{i=1}^{N} c\left[ v_{ij}\left( \frac{d_{ij}}{c_{ij}} = \max \right) \right]$.

Необходимыми исходными данными для решения задачи выбора многоверсионной технологии разработки ИУС в любой постановке является модель жизненного цикла многоверсионной ИУС, включающая:

– множество этапов ЖЦ, $E = \{E_i\}$, $i = 1,\ldots,N$;

– для каждого i-го этапа ЖЦ – множество СВВИ, $MV_i = \{MV_{ij}\}$, $i = 1,\ldots,M_i$;

– для каждого из СВВИ – значения метрики диверсности $d_{ij}$ и стоимости $c_{ij}$ (приращение стоимости по сравнению с одноверсионным вариантом $i$-го этапа ЖЦ ИУС).

## Выводы

Полученные решения для вариантов задачи оптимального выбора являются основой метода выбора многоверсионных технологий разработки ИУС. Данный метод применялся при разработке диверсного программно-технического комплекса системы аварийной и предупредительной защиты реактора (ПТК АЗ-ПЗ) [15].

Предложенный вид программно-аппаратного разнообразия заключается в применении элементной базы от разных производителей, различных

программируемых компонентов (микропроцессоров и ПЛИС), различных языков программирования (Assembler и C). Значения метрик диверсности для различных видов разнообразия получены в работе [9]. Реализация диверсности позволило на порядок по сравнению с одноверсионной системой снизить интенсивность отказов, вызванных проявлением дефектов проектирования.

Полученные в данной статье результаты применимы для любых видов диверсности ИУС. Ограничения, связанные с взаимосвязью отдельных способов внесения версионной избыточности на различных этапах ЖЦ, учитываются путем удаления соответствующих ребер из полносвязной графовой модели ЖЦ ИУС (рис. 1).

## Литература

1. Avizienis A., Lapri J.-C. Dependable Computing: From Concepts to Design Diversity // Proceedings IEEE, 1986. – Vol. 74, n. 5. – P. 8-21.

2. Littlewood B., Strigini L. A discussion of practices for enhancing diversity in software designs // Technical report. Centre for Software Reliability, London (UK). – 2000. – 55 p.

3. Laprie J.-C. Dependability Handbook. LAAS Report n 98-346. – Toulouse: Laboratory for Dependability Engineering, 1998. – 365 p.

4. Харченко В.С., Жихарев В.Я., Илюшко В.М., Нечипорук Н.В. Многоверсионные системы, технологии. – Х.: НАКУ им. Н.Е. Жуковского «ХАИ», 2003. – 486 с.

5. Preckshot G.G. Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems. – Livermore, USA: Lawrence Livermore National Laboratory, 1994. – 45 p.

6. Волковой А.В., Скляр В.В., Харченко В.С. Исследование зависимости “надёжность-стоимость” при использовании многоверсионных технологий разработки программных средств // Авіаційно-космічна техніка і технологія. – Х.: НАКУ ім. Н.Є. Жуковського «ХАІ», 2002. – Вип. 35. – С. 182-186.

7. Скляр В. В. Анализ метрик диверсности программного обеспечения // Электронное моделирование. – 2004. – № 26. – С. 95-104.

8. Харченко В.С., Пискачева И.В., Скляр В.В. Метрики диверсности: Классификация, анализ и применение для оценки надежности и безопасности компьютерных систем управления // Открытые информационные и компьютерные интегрированные технологии.– Х.: НАКУ им. Н.Е. Жуковского «ХАИ». – 2001. – № 9. – С. 194-214.

9. Головир В.А., Скляр В.В., Харченко В.С. Методы внесения и оценки версионной избыточности при разработке информационно-управляющих систем на базе ПЛИС // Вісник Хмельницького національного університету. – 2005. – № 4, ч. 1, т. 1.– С. 94-97.

10. Волковой А.В., Скляр В.В., Харченко В.С. Метод формирования моделей многоверсионного жизненного цикла для программных проектов // Інформаційно-керуючі системи на залізничному транспорті. – 2004. – № 2. – С. 40-44.

11. Конюховский П.В. Математические методы исследования операций в экономике. – С.-Пб.: Питер, 2000. – 208 с.

12. Фурман І.О., Краснобаєв В.А., Рожков П.П. та ін. Автоматизовані системи керування технологічними процесами. – Х.: Факт, 2006. – 317 с.

13. Зайченко Ю.П., Шумилова С.А. Исследование операций. – К.: Вища школа, 1990. – 239 с.

14. Горбатов В.А. Теория частично упорядоченных систем. – М.: Советское радио, 1976. – 336 с.

15. Бахмач Е.С., Виноградская С.В., Розен Ю.В. и др. Программно-технические комплексы аварийной и предупредительной защиты ядерных реакторов: обеспечение и оценка безопасности // Ядерная и радиационная безопасность. – 2005. – Т. 8, № 1. – С. 21-50.

*Поступила в редакцию 2.02.2007*

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