

УДК 621.039:004.05

## Модели многоверсионных вычислений и их обобщение для отказоустойчивых систем

А. А. Сиора, В. С. Харченко

*Научно-производственное предприятие "Радий", Украина**Национальный аэрокосмический университет**имени Н. Е. Жуковского "ХАИ", Украина*

В статье описываются теоретико-множественные и структурно-автоматные модели различных типов многоверсионных систем обработки информации (МВС). Исследуются свойства мультидиверсных и адаптивных МВС, а также МВС, в которых используются диверсные системы счисления. Показано, что предложенные модели обобщают классы отказоустойчивых вычислений, базирующихся на структурной, временной и версионной избыточности.

**Ключевые слова:** многоверсионные системы, структурно-автоматные модели, отказоустойчивые вычисления, версионная, структурная и временная избыточность.

В статі описуються теоретико-множинні та структурно-автоматні моделі різних типів багатверсійних систем обробки інформації (БВС). Досліджуються властивості мультидиверсних і адаптивних БВС, а також БВС, у яких використовуються диверсні системи счислення. Показано, що запропоновані моделі узагальнюють класи відмовостійких обчислень, що базуються на структурній, часовій та версійній надмірності.

**Ключові слова:** багатверсійні системи, структурно-автоматні моделі, відмовостійкі обчислення, структурна, часова і версійна надмірність.

The set-theoretical and structure-automaton models of the different sorts of multi-version data processing systems (MVS) are described. The properties of multi-diversion and adaptive MVSs and MVSs based on the diversity of numeral systems are researched. The proposed models are a generalization of fault-tolerant computing using structure, temporary and version redundancy.

**Key words:** multi-version systems, structure-automaton models, fault-tolerant computing, structure, temporary and version redundancy.

### 1. Общая постановка задачи и её актуальность

Многоверсионные вычисления (обработка информации и управление объектами различной природы), базирующиеся на использовании двух и более программно-аппаратных версий для реализации каналов резервированной системы, применяются для обеспечения устойчивости к проектным и физическим дефектам. Идея многоверсионных вычислений, высказанная в [1], экспериментально исследованная в [2], получила распространение во многих областях, прежде всего, так называемых критических системах, где цена отказа является очень высокой [3-5]. Для таких систем, например, систем аварийной защиты реактора атомных станций, требование по использованию версионной избыточности и реализации многоверсионных вычислений является нормативным [4].

Ключевые проблемы многоверсионных вычислений – определение и выбор видов версионной избыточности, разработка многоверсионных систем (МВС), а также оценка реального уровня диверсности (многоверсионности). Развитие технологий, увеличение числа видов диверсности и вариантов

архитектурирования расширяет возможности по созданию МВС и требует совершенствования их модельной базы. Кроме того, важным представляется анализ соотношения между многоверсионными вычислениями и отказоустойчивыми вычислениями в целом.

Таким образом, общая задача формулируется как разработка моделей МВС, в которых используются различные виды версионной и других видов избыточности, способов адаптации, и их обобщение как отказоустойчивых систем.

## 2. Истоки исследования авторов

Данная работа базируется на ряде моделей и результатов, полученных в [5-21]. Исходная идея для разработки модели и собственно понятие "многоверсионной" или "многоальтернативной" системы были определены в [6,7]. В этих работах получены вероятностные оценки надежности для МВС с учетом безотказности программных и аппаратных средств.

Комплексное решение проблемы многоверсионных вычислений и соответствующие модели были предложены в [8], где сформировались теоретическая база МВС, в которых применялся один вид версионной избыточности, понятие многоверсионной технологии (МВТ), а также методическое обеспечение для их выбора. Формальное представление МВТ было дано далее в [9], а в [10] на базе моделей многоверсионных систем и технологий введено понятие и разработана модель многоверсионного проекта.

Парадигма "гарантоспособной системы из негарантоспособных компонент" и различные аспекты ее реализации посредством МВТ исследованы применительно к компьютерным системам [11] и инфраструктурам [12].

Модель МВС как  $(n,m)$ -версионной системы, в которой используется несколько видов версионной избыточности, предложена в [13]. Такие системы получили название мультидиверсных (МДВС). МВС, в которых используется диверсность систем счисления (позиционных и непозиционных), их модели, архитектуры и соответствующие МВТ исследованы в [5].

Таксономия многоверсионных вычислений сформировалась в [13-15]. В [14] базовые понятия многоверсионных вычислений проанализированы и развиты в контексте таксономии гарантоспособных и так называемых резистивных систем (resilient systems), а также свойства самоэволюционирования (self-evolvability).

В [5,13], проанализированы классификационные схемы версионной избыточности, введено понятие "куба диверсности", а затем в [15,16] они детализированы для МВС на программируемой логике. В [17], кроме того, дан обзор методов оценки диверсности и областей применения многоверсионных вычислений в различных критических и бизнес-критических приложениях.

Отдельное направление исследований связано с безопасными (в информационном смысле) многоверсионными вычислениями (multi-version secure computing) [17-21]. В рассматриваемом контексте важными являются результаты систематизации проблем на стыке "информационная безопасность-многоверсионность-отказоустойчивость" [18] и предложений по их решению [19], включая архитектуры МВС, устойчивые к дефектам взаимодействия, вызванным информационными воздействиями предложенная [20,21].

### 3. Нерешенные проблемы и цель работы

Анализ известных публикаций позволяет сделать следующие выводы.

1. В ключевых работ [1,22], где была предложен и развит принцип N-версионного программирования (проектирования), как подход к снижению рисков отказов, вызванных программными (проектными) дефектами, а также работах B.Littlewood, L. Strizini, P. Popov [23,24] F. Saglietti [25], L. Pullum [26] и др., в которых исследованы методы внесения версионной избыточности и оценки вероятности отказов, понятие и формальные модели МВС как особого вида отказоустойчивых систем не рассматривались.

2. В [27] и других работах, где исследуется класс отказоустойчивых мажоритарных систем (так называемых  $(k,n)$ -систем,  $n$  число каналов,  $k$  порог мажоритирования), не учитывается возможность их многоверсионной реализации. В то же время модели многоверсионных мажоритарных систем, исследованные в [8-10], не полностью описывают множество возможных решений, полученном как декартово произведение множеств  $(M_{\text{МВС}} \times M_{(k,n)\text{-систем}})$ .

3. В публикациях авторов данной работы, проанализированных выше, не систематизированы и детализированы в полной мере модели МВС, учитывающие возможности совместного использования нескольких видов версионной избыточности, а также других видов избыточности, включая временную, информационную.

В связи с этим **целью** данной статьи является разработка и теоретическое обобщение моделей многоверсионных вычислений как класса отказоустойчивых вычислений.

## 4. Теоретико-множественные модели МВС

### 4.1. Базовые модели МВС

Как известно [8], одноверсионная  $W(1)$  и многоверсионная система  $W(n)$  описываются четверкой и шестеркой соответственно:

$$W(1) = \{X, Y, Z, \Phi\}, \quad (1)$$

$$W(n) = \{X, Y, Z, \Phi, V, \Psi\}, \quad (2)$$

где  $X$  – множество (алфавит) входных сигналов;

$Y$  – множество (алфавит) внутренних состояний;

$Z$  – множество (алфавит) выходных сигналов;

$\Phi = \{\varphi_i, i=1, \dots, a\}$  – множество выполняемых функций;

$V = \{v_j, j=1, \dots, n\}$  – множество версий;

$\Psi = \{\psi_s, s=1, \dots, \vartheta\}$  – множество вариантов обработки результатов выполнения версий.

С учетом (1,2) многоверсионная система  $W(n)$  и одноверсионная  $W(1)$  связаны зависимостью

$$W(n) = \{W(1), V, \Psi\}. \quad (3)$$

Одноверсионная  $W(1)$  может быть структурно избыточной и содержать обычные средства  $\Psi$ , осуществляющие обработку информации от идентичных каналов. В этом случае множество  $V$  является вырожденным ( $card V=1$ ).

Функции  $\varphi_i \in \Phi$  задают отображение входного алфавита  $x_r \subset X$  на алфавит внутренних состояний  $y_l \subset Y$  и выходной алфавит  $z_k \subset Z$ . В свою очередь, элементам  $v_j \subset V$  соответствует множество версий для функций  $\varphi_i \in \Phi$ :

$$\forall \varphi_i \sim v_j = \{v_{ij}, j=1, \dots, n_i\}.$$

Для системы  $W(n)$  справедливо:

$$\forall j = \overline{1, \hat{a}} : \exists j : n_j > 1.$$

Если выполняется функция  $\varphi_i$  на версии  $v_{ij}$ , то соответствующие выходные сигналы (алфавит) обозначаются  $z_i(v_{ij})$ . Тогда для каждой функции  $\varphi_i$  элемент  $\psi_s \in \Psi$  задает вариант отображения подалфавита  $z_i(v_{ij})$  в выходной алфавит  $Z_i^{(s)}$ :

$$\psi_s : \{z_i(v_{i1}), \dots, z_i(v_{in_i})\} \rightarrow Z_i^{(s)}.$$

Отображение  $\psi_s$  в общем случае характеризуется:

- подмножеством версий  $\Delta v_s \subset v_j$ , используемым для получения выходного сигнала  $Z_i$ ;

- вектором  $\overline{t}_s$  времени инициализации версий  $v_{ij}$ :

$$\overline{t}_s = \{t(v_{i1}), \dots, t(v_{in_i})\};$$

- способом преобразования  $\eta_s$  значений  $z_i(v_{i1}), \dots, z_i(v_{in_i})$  в выходной сигнал  $Z_i^s$ .

Таким образом,

$$\forall \psi_s \in \Psi : \psi_s = \{ \Delta v_s, \overline{t}_s, \eta_s \}. \quad (4)$$

С учетом сказанного имеем:

$$Z_i^{(s)} = \eta_s [z_i(v_{ij}), \overline{t}_s], \quad v_{ij} \in \Delta v_s. \quad (5)$$

Способы преобразования  $\eta_s$  могут быть следующими:

1) конъюнктивными, когда  $Z_i^s = \bigvee z_i(v_{ij})$ ;

2) конъюнктивно-временными, когда  $Z_i^s = \bigvee z_i(v_{ij}) \sigma_{ij}$ , где  $\sigma_{ij}=1$ , если  $t=t(v_{ij})$ , в противном случае  $\sigma_{ij}=0$ ;

3) мажоритарными, когда  $Z_i^s = M[z_i(v_{ij})]$ , где  $M$  – функция мажоритирования  $k$  из  $l$  (или  $k$  из  $n$ );

4) мажоритарно-взвешенными, когда дополнительно задаются веса версий  $\omega(v_{ij})$ , учитываемые при мажоритировании;

5) функциональными, когда  $Z_i^s = f[z_i(v_{ij})]$ , где  $f$  – некоторая функция преобразования результатов выполнения версий.

Модель (2) описывает систему с  $n$  версиями, где  $n = \sum_{i=1}^a n_i$ .

При этом она не учитывает возможность применения нескольких видов версионной избыточности. Их множество  $R = \{r_d, d=1, \dots, m\}$  может быть декомпозировано на подмножества по версиям продуктов  $v_{prd}(t_j)$  и процессов  $v_{prc}(t_j)$ :

$$R = (\bigcup_j \Delta R_{prdj}) \cup (\bigcup_j \Delta R_{prcj}), \quad (6)$$

где  $\Delta R_{prdj}$  и  $\Delta R_{prcj}$  – соответствующие подмножества.

Тогда справедливо, что

$$m \leq \sum_j m_{prdj} + \sum_j m_{prcj}, \quad (7)$$

где  $m_{prdj}$  и  $m_{prcj}$  – мощности подмножеств  $\Delta R_{prdj}$  и  $\Delta R_{prcj}$  соответственно.

В итоговых версиях продуктов многоверсионной системы таким образом аккумулируются различные виды версионной избыточности  $r \in R$ . Это описывается специальным отображением

$$\Theta: R \rightarrow V, \quad (8)$$

описываемым в матричной форме  $\Theta = \|\theta_{dj}\|$ ,  $d = \overline{1, m}$ ,  $j = \overline{1, n}$ ,

$$\theta_{dj} = \begin{cases} 1, & \text{если вид ВП } r_p \text{ используется в версии } v_j; \\ 0, & \text{в противном случае.} \end{cases}$$

Тогда мультидиверсная или многоверсионная  $W(n, m)$  система описывается выражением

$$W(n, m) = \{X, Y, Z, \Phi, V, \Psi, R, \Theta\}. \quad (9)$$

или

$$W(n, m) = \{W(n), R, \theta\}. \quad (10)$$

С учетом (2), (9), (10) имеем

$$W(n, m) = \{W(1), V, \Psi, R, \theta\}. \quad (11)$$

Для многоверсионных систем обработки информации важно также задать соответствие между множествами версий  $V$  и резервных каналов системы  $C = \{c_q, q=1, \dots, l\}$ . Оно задается отображением

$$Q: V \rightarrow C, \quad (12)$$

которое также описывается булевой матрицей  $Q = \|\omega_{gj}\|$ ,  $d = \overline{1, m}$ ,  $g = \overline{1, l}$ , где

$$\omega_{gj} = \begin{cases} 1, & \text{если версия } v_j \text{ реализуется в резервном канале } c_j; \\ 0, & \text{в противном случае.} \end{cases}$$

Тогда имеем модель многоверсионной системы в следующем виде:

$$W(n, m, l) = \{X, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q\}. \quad (13)$$

По аналогии с (3,10,11) имеем:

$$W(n,m,l) = \{ W(n), R, \Theta, C, Q \} = \{ W(n,m), C, Q \}. \quad (14)$$

#### 4.2. Модели МВС с временной и информационной избыточностью

**Утверждение.** Выражение (13) и его вариант, когда  $R = \phi$ , описывают мультидиверсную и немультидиверсную МВС с временной избыточностью.

*Доказательство.* Матрица  $\| \omega_{jg} \|$ , задающая отображение  $Q$ , не накладывает ограничение на число единичных элементов, содержащихся в столбце. Если  $\sum_{g=1}^l \omega_{jg} = 1$ , то в одном канале реализуется одна версия. Если

$\sum_{g=1}^l \omega_{jg} > 1$ , это означает, что версия реализуется в канале  $C_g$  несколько раз. Такая

же ситуация справедлива для случая немультидиверсной МВС. Последовательность выполнения версий в канале может быть задана посредством параметров вектора  $\bar{t}_s$  функции  $\Psi$ . Следовательно, выражение (13) и выражение

$$W(n,m,l) = \{ X, Y, Z, \Phi, V, \Psi, C, Q \} \quad (15)$$

описывают систему с временной избыточностью. *Утверждение доказано.*

Рассмотрим варианты МВС с разными видами избыточности, используемой совместно с версионной.

1. Если в системе не используется временная избыточность, в одном канале не хранится несколько версий, то  $l \geq n$ . При  $l = n$  имеем систему  $W(n, m, n)$ , которую будем называть симметричной МВС.

2. Если в каналах хранится несколько версий, которые могут выполняться последовательно во времени, имеем систему с версионно-структурно-временной избыточностью. Тогда возможно, что  $l < n$ .

Многоверсионные системы, в которых применяется временная избыточность, будем обозначать как  $W(n, m, n, p)$ , разделяя число версий, реализуемых параллельно за счет структурной избыточности  $n_c$ , и версий, реализуемых последовательно во времени на одном канале  $n_g$  с  $p$  повторами.

3. Если  $\eta_s$  – функция мажоритирования и многоверсионная система обработки информации относится к классу мажоритарных, то возможно несколько вариантов ее представления:

а) " $k$  из  $l$ "; в этом случае порог мажоритирования задаются по числу (по большинству) работоспособных каналов и имеем систему  $W(n, m, l/k)$ ;

б) " $k$  из  $n$ "; в этом случае порог мажоритирования задаются по большинству версий и имеем систему  $W(n/k, m, l)$ ;

в) различные варианты адаптивных схем, определяемые фактическим состоянием каналов и версий.

4. Для описания адаптивных многоверсионных систем, в которых способ преобразования (функции)  $\eta_s$  не сводится к обычным логическим операциям,

операціям простого или взвешенного мажоритирования, а требуется задания более сложного алгоритма адаптации, необходимо специальное описание всех параметров, входящих в функцию  $\Psi$ , и  $\Delta\eta_s$ , и  $\bar{t}_s$ , и  $\eta_s$ . В этом случае будем обозначать ее как  $\Psi_A$ , и соответствующую систему  $W_A$  описывать в виде:

$$W_A(n,m,l) = \{X, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q\}. \quad (16)$$

5. Множество входных сигналов системы  $X$  может быть декомпозировано по версиям, когда справедливо

$$X = \bigcup_j \tilde{O}_j,$$

$$\forall j_1, j_2 \in \overline{1, n}, j_1 \neq j_2: X_{j_1} \cap X_{j_2} = \emptyset, \tilde{O}_{j_1} \cap \tilde{O}_{j_2} = \emptyset.$$

Такие системы будем называть МВС с естественно разделенным входным алфавитом,

$$W_{EX} = \{ \{X_j\}, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q \}. \quad (17)$$

Если версии обрабатывают информацию, представленную в разной форме (разных системах счисления), такие системы будем называть МВС с искусственно разделенным входным алфавитом  $W_{IX}$ .

Для их описания должна быть задана функция преобразователя  $P_x$  (или преобразователей  $P_{x_j}$ ) в дополнение ко входному алфавиту  $X$ :

$$W_{IX} = \{X, \{P_{x_j}\}, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q\}. \quad (18)$$

## 5. Структурно-автоматные модели

Представим структурно-автоматные модели для основных классов МВС с учетом введенных выше множеств и отображений  $\Theta$ ,  $Q$ ,  $\Psi$ . Уточним виды этих отображений для различных классов систем.

### 5.1. Системы $W(n,m,l,p)$

Данные МВС являются наиболее общим типом систем, в которых используются три вида избыточности: версионная, структурная и временная (рис.1,а). Кроме того, эта система является мультидиверсной, поскольку в ней используется  $m$  видов версионной избыточности.

Каждый из каналов  $C_q$ ,  $q=1, \dots, l$ , в общем случае представляет собой автомат с памятью  $AC_q$ , описываемый:

- автоматным временем  $t$ ;
- множествами входных  $x_q(t) \subset X$ , выходных сигналов  $z_{q\tau}(t)$ , состояний памяти  $y_q(t) \subset Y$ , включая начальное  $y_{q0}$  при  $t=0$ ;
- функциями переходов  $A_q$  и выходов  $\Gamma_q$ .

Для системы в целом автоматная модель представляется соответствующими алфавитами, функцией переходов, получаемой как  $A = \Psi(A_q)$ , а также функции выходов  $\Gamma$  как конкатенации функций  $\Gamma_q$  [8].

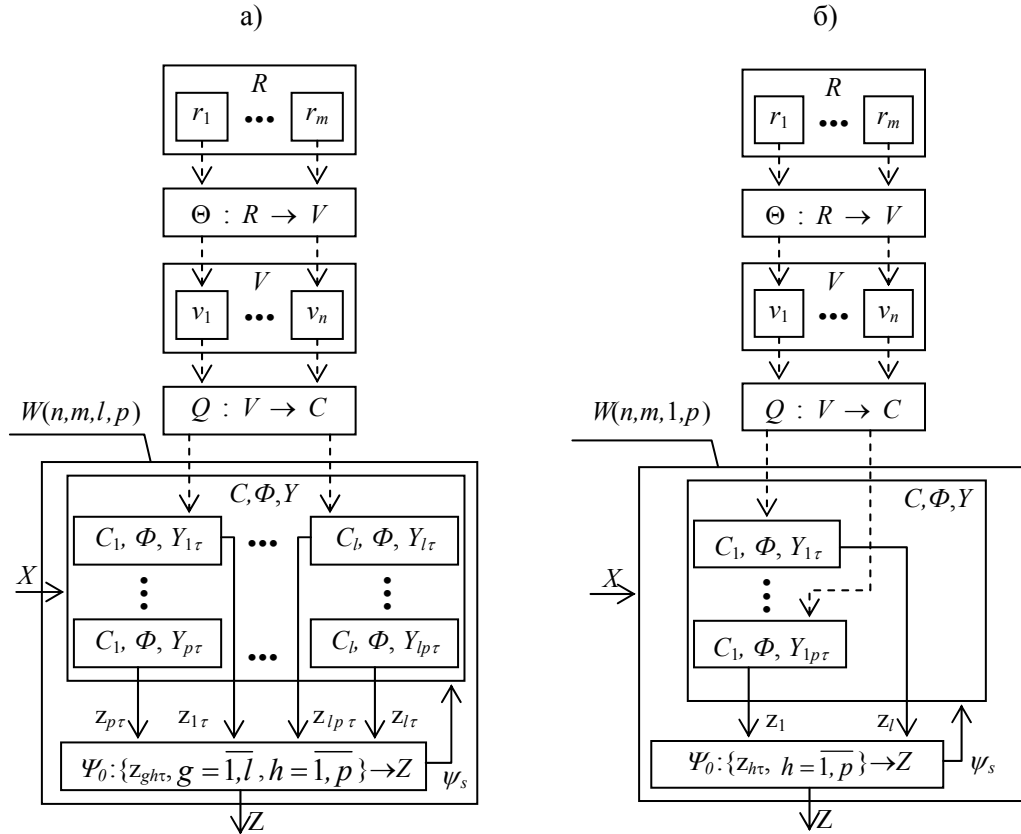


Рис. 1. Модели систем  $W(n,m,l,p)$  (а),  $W(n,m,1,p)$  (б)

Для системы на Рис.1,б  $l = 1$ , т.е. МВС реализуется на одном физическом канале (версионно-временная избыточность).

## 5.2. Системы $W(n,m,l)$

Данные МВС обобщают системы, в которых используются версионная и структурная избыточность. На Рис.2 представлены модели систем  $W(n,m,l)$  (а),  $W_{IX}(n,m,l)$  (б),  $W_{EX}(n,m,l)$  (в),  $W(n,l,l)$  (г). Они описываются выражениями (13), (17), (18) и выражением (2) соответственно.

## 6. МВС как обобщение отказоустойчивых систем

В Табл. 1 приведены результаты сопоставительного анализа МВС как отказоустойчивых систем. Разработанные модели МВС соотнесены с известными классами отказоустойчивых систем, используя введенную систему обозначений для МВС  $W, W_A, W_{EX}, W_{IX}$ .

Свойства ДФ- и ДП-устойчивости для разных типов систем определяются исходя из возможности парировать отказы, обусловленные соответственно физическими дефектами и дефектами проектирования. Парирование последних возможно только в многоверсионных системах (МВС и МДВС).



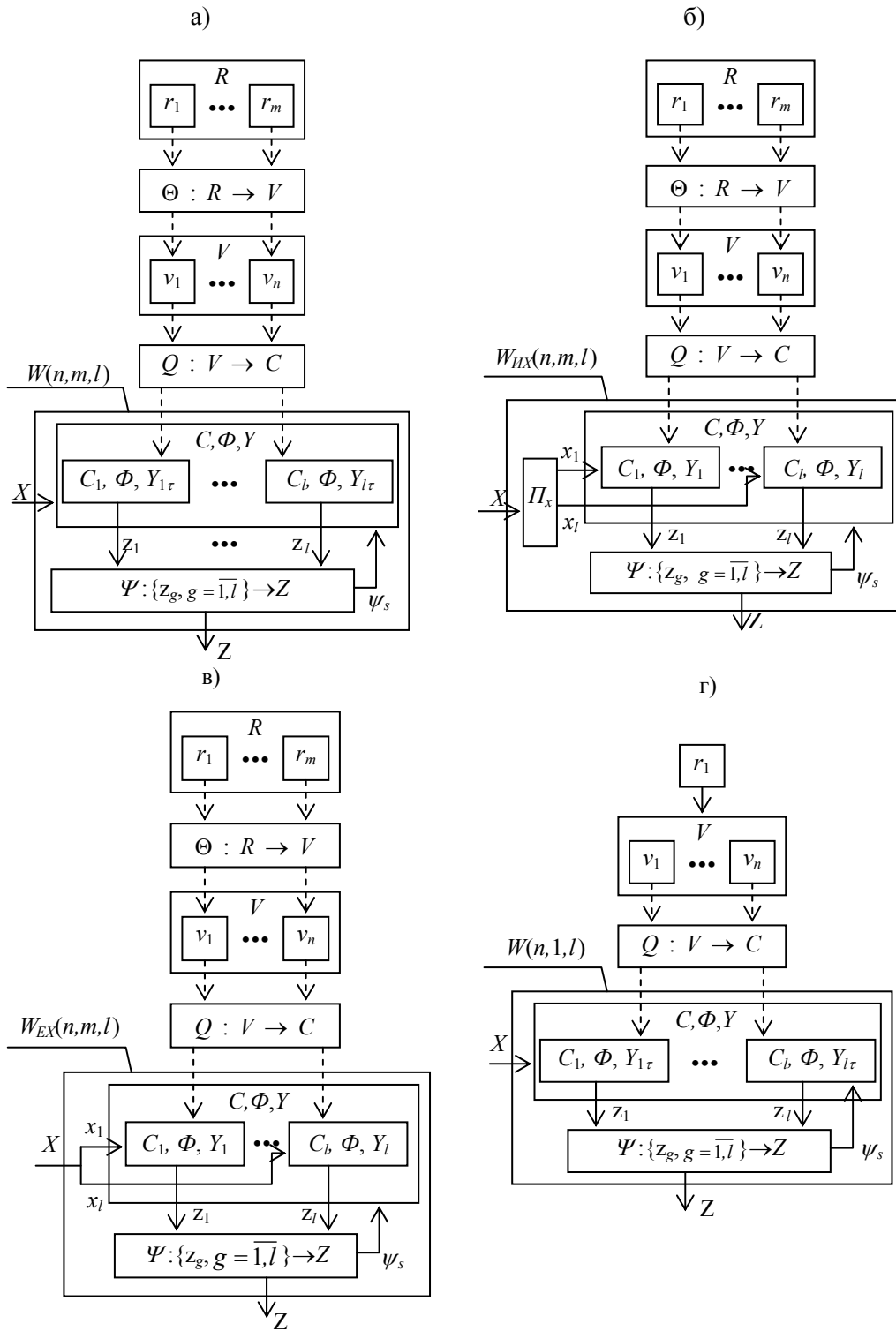


Рис. 2. Модели систем  $W(n,m,l)$  (а),  $W_{HX}(n,m,l)$  (б),  $W_{EX}(n,m,l)$  (в),  $W(n,1,l)$  (г)

Таблица 1. МВС как отказоустойчивые системы

№ п/п	Модель	Тип системы	Класс системы
1	$W(1, 0, 1)$	ОВС	Нерезервированная неотказоустойчивая
2	$W(1, 0, l)$	ОВС	Резервированная ДФ-устойчивая
3	$W(1, 0, l/k)$	ОВС	Мажоритарная ДФ-устойчивая
4	$W(1, 0, 1, p)$	ОВС	Резервированная (с временной избыточностью) ДФ- и ДП-устойчивая
5	$W(1, 0, 1, p/k_e)$	ОВС	Резервированная (с временной избыточностью) ДФ- и ДП-устойчивая
6	$W(1, 0, l, p/k_e)$	ОВС	Резервированная (с временной избыточностью) ДФ- и ДП-устойчивая
7	$W(1, 0, l/k, p/k_e)$	ОВС	Резервированная (с временной избыточностью) ДФ- и ДП-устойчивая
8	$W_A(1, 0, l/k, p/k_e)$	ОВС	Резервированная (с временной избыточностью) ДФ- и ДП-устойчивая
9	$W_A(1, 0, l/k)$	ОВС	Адаптивная ДФ-устойчивая
10	$W(1+n_e, 1, 1, p)$	МВС	Резервированная (с временной избыточностью) ДП-устойчивая
11	$W(1+n_e, 1, 1, p/k_e)$	МВС	Мажоритарная ДФ-устойчивая
12	$W_A(1+n_e, 1, 1, p/k_e)$	МВС	Адаптивная ДФ-устойчивая
13	$W(1+n_e, m, 1, p)$	МДВС	Резервированная (с временной избыточностью) ДП-устойчивая
14	$W(1+n_e, m, 1, p/k_e)$	МДВС	Адаптивная ДФ-устойчивая
15	$W_A(1+n_e, m, 1, p/k_e)$	МДВС	Адаптивная ДФ-устойчивая
16	$W(n_c, 1, l, 0)$	МВС	Резервированная ДФ- и ДП-устойчивая
17	$W(n_c, 1, l/k, 0)$	МВС	Мажоритарная ДФ- и ДП-устойчивая
18	$W_A(n_c, 1, l/k, 0)$	МВС	Адаптивная ДФ- и ДП-устойчивая
19	$W(n_c, m, l, 0)$	МДВС	Резервированная ДФ- и ДП-устойчивая
20	$W(n_c, m, l/k, 0)$	МДВС	Мажоритарная ДФ- и ДП-устойчивая
21	$W_A(n_c, m, l/k, 0)$	МДВС	Адаптивная ДФ- и ДП-устойчивая
22	$W(n_c+n_e, 1, l, p)$	МВС	Резервированная ДФ- и ДП-устойчивая (с временной избыточностью)
23	$W(n_c+n_e, 1, l, p/k_e)$	МВС	Мажоритарно-резервированная ДФ- и ДП-устойчивая (с временной избыточностью)
24	$W_A(n_c+n_e, 1, l, p/k_e)$	МВС	Адаптивная ДФ- и ДП-устойчивая (с временной избыточностью)
25	$W(n_c+n_e, m, l, p)$	МДВС	Резервированная ДФ- и ДП-устойчивая (с временной избыточностью)
26	$W(n_c+n_e, m, l/k, p/k_e)$	МДВС	Мажоритарная ДФ- и ДП-устойчивая (с временной избыточностью)
27	$W_A(n_c+n_e, m, l/k, p/k_e)$	МДВС	Адаптивная ДФ- и ДП-устойчивая (с временной избыточностью)
28	$W_{EX}(n, m, l, 0)$	МДВС	Резервированная ДФ- и ДП-устойчивая с естественно разделенными вх. сигналами
29	$W_{IX}(n, m, l, 0)$	МДВС	Резервированная ДФ- и ДП-устойчивая с искусственно разделенными вх. сигналами

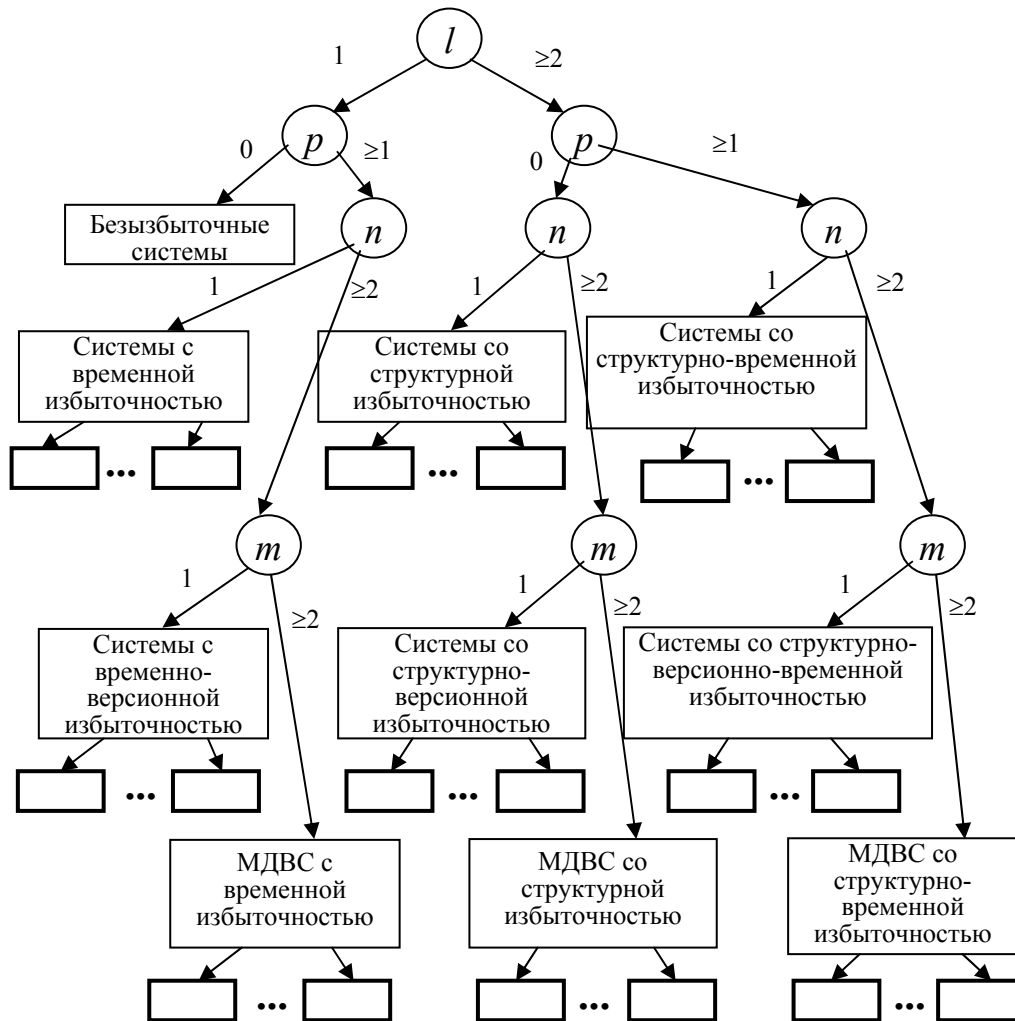


Рис.3. Дерево вариантов МВС как отказоустойчивых систем

### 7. Выводы. Направления дальнейших исследований

Парадигма многоверсионности эволюционировала в течение сорока лет от своей начальной идеи  $N$ -версионного программирования к комплексу теоретических методов, средств и технологий анализа и синтеза многоверсионных систем, применяемых для многих критических приложений и обеспечивающих существенное повышение гарантоспособности и ее составляющих свойств – безотказности, функциональной и информационной безопасности.

В данной работе получены и систематизированы модели различных классов МВС, в которых наряду с версионной и структурной используются и другие виды избыточности (временная, информационная). Исследованы свойства этих МВС как отказоустойчивых систем. На Рис.3 представлено дерево вариантов МВС в зависимости от значения параметров  $l, p, n, m$ .

Дальнейшие исследования целесообразно направить на разработку методов количественной оценки и синтеза мультидиверсных систем с комбинированной избыточностью с учетом требований реальных проектов.

#### ЛИТЕРАТУРА

1. Avizienis A., Lapri J.-C. Dependable Computing: From Concepts to Design Diversity // Proceedings IEEE. – 1986, Vol. 74, № 5. – P. 8–21.
2. Knight J.C., Leveson N.G. An experimental evaluation of the assumption of independence in multi-version programming // IEEE Trans. Soft. Eng. – 1986, vol. SE-12, № 1. – P.96-109.
3. Wood R., Belles R., Cetiner M., et.al. Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems. NUREG/CR-7007, ORNL/TM-2009/302. - NRC Job Code N6176, 2009. – 225 p.
4. Сиора А.А., Краснобаев В.А., Харченко В.С. Отказоустойчивые системы с версионно-информационной избыточностью / Под ред. Харченко В.С. – Мин. образов. и науки Украины, Нац. аэрокосм. ун-т «ХАИ», 2009. – 321 с.
5. Ястребенецкий М.А., Васильченко В.Н., Харченко В.С. и др. Информационно-управляющие системы АЭС: проблемы безопасности. - Киев: Техника, 2004. – 472 с.
6. Харченко В.С., Паршин В.В. Многоверсионные системы и обеспечение гарантоспособности. Препринт №321. – Х.: ИПМ АНУ, 1989. – 33 с.
7. Харченко В.С., Паршин В.В. Гарантоспособные вычислительные системы с последовательно-параллельным выполнением версий. Препринт №329. – Х.: ИПМ АНУ, 1990. – 31 с.
8. Харченко В.С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. – Х.: Мин. обороны Украины, 1996. – 503 с.
9. Kharchenko V.S. Multiversion Systems: Models, Reliability, Design Technologies // Proceeding of 10<sup>th</sup> European Conference on Safety and Reliability, Munich, Germany, 13-17 September, 1999, vol. 1. – P.73-77.
10. Харченко В.С., Жихарев В.Я., Илюшко В.М. и др. Многоверсионные системы, технологии, проекты. – Нац. аэрокосм. ун-т «ХАИ». – 486 с.
11. Kharchenko V.S., Sklyar V.V., Volkoviy A.V. Multi-version Information Technologies and Development of Dependable Systems out of Undependable Components //Proc. of International Conference of Dependability of Computer Systems, DepCoS–RELCOMEX2007, IEEE Computer Society, 2007. – P. 43–50.
12. Kharchenko V., Sklyar V., Odaruschenko O., Dependable Computing Systems for Supporting Transformation of the Force Information Infrastructure // Information & Security. Switzerland. – 2007, vol.22. – P. 75-91.
13. Сиора А.А., Скляр В.В., Харченко В.С. (n,m)-версионные системы: таксономия, модели, технологии // Вісник Харківського Національного університету №833. Серія "Математичне моделювання, інформаційні технології автоматизованих систем управління"- Вип.10, 2008. – С.231-241.
14. Харченко В.С. Гарантоздатні системи та багатOVERсійні обчислення:аспекти еволюції// Радіоелектронні та комп'ютерні системи, 2009, №7. – С. 12-27.

15. Kharchenko V.S., Siora A.A., Bakhmach E.S. Diversity-Scalable Decisions for FPGA-based Safety-Critical I&Cs: from Theory to Implementation // Proceedings of NPIC&HMIT 2009, Knoxville, USA, April 5-9, 2009.
16. Kharchenko V.S., Bakhmach E.S., Siora A.A. et.al. Diversity-Oriented FPGA-Based NPP I&C Systems: Safety Assessment, Development, Implementation // Proceedings of the 18<sup>th</sup> International Conference on Nuclear Engineering, ICONE18, Xi'an, China May 17-22, 2010.
17. Волковой А.В., Лысенко И.В., Харченко В.С., Шурыгин О.В. Многоверсионные системы и технологии для критических приложений. Лекции / Под ред. Харченко В.С. – Мин. образов. и науки Украины, Нац. аэрокосм. ун-т «ХАИ», 2008. – 221 с.
18. Elyasi Komari I., Kharchenko V., Romanovsky A., Babeshko E. Diversity and Security of Computing Systems: Points of Interconnection. Part 1: Introduction to Methodology // MASAUM Journal of Open Problems in Science and Engineering (MJOPSE). – MASAUM Network, 2009, vol.1, № 1. – P. 28–32.
19. Elyasi Komari I., Kharchenko V., Romanovsky A., Babeshko E., Lysenko I. Diversity and Security of Computing Systems: Points of Interconnection. Part 2: Methodology and Case Study// MASAUM Journal of Open Problems in Science and Engineering (MJOPSE). – MASAUM Network, 2009, vol.1, № 1. – P. 33-41.
20. Gorbenko A., Kharchenko V., Tarasyuk O, Furmanov A. F(I)MEA-Technique of Web-services Analysis and Dependability Ensuring. LNCS 4157. Rigorous Development of Complex Fault-Tolerant Systems/ Butler M., Jones C., Romanovsky A., Trubitsyna E. (eds.). Springer, 2006. – P.153–168.
21. Kharchenko V., Romanovsky A., Gorbenko A. Using Inherent Service Redundancy and Diversity to Ensure Web Services Dependability In M. Butler, C. Jones, A. Romanovsky, E. Troubitsyna (Eds.) “Methods, Models and Tools for Fault Tolerance”, LNCS 5454, Springer, 2009.– P. 324-341.
22. The Evolution of fault-tolerant computing / A. Avizienis, H. Kopetz, J.C. Laprie (eds.). – Wien, New York: Springer-Verlag, 1987. - 463 p.
23. Littlewood B., Popov P. Modelling the effects of combining diverse software fault removal techniques // IEEE Transactions on Software Engineering. – 2000. – SE-26(12). – P. 1157-1167.
24. Littlewood B., Strigini L. A discussion of practices for enhancing diversity in software designs // Technical Keport. Centre for Software Reliability, London UK, 2000. – 55 p.
25. Saglietti F. The Impact of Forced Diversity on the Failure Behaviour of Multi-version Software in "Automatisierungs- und Leitsysteme in den neunziger Jahren" Proc. Fachtagung Prozeßrechnungssysteme '91 Berlin, Germany. – Informatik-Fachberichte Nr. 269, Springer-Verlag, Berlin 1991. – P.193 – 205.
26. Pullum L. Software fault tolerance techniques and implementation. – Artech House computing library, 2001. – 343 p.
27. Boland P., Proshan F. The Reliability of K Out of N Systems // The Annals of Probability, vol II, No3, 1983. – P.760-784.

---

Надійшла у першій редакції 04.02.2010, в останній - 10.04.2010.

© А. А. Сиора, В. С. Харченко, 2010