## КАТАСТРОФОУСТОЙЧИВЫЕ КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕРВИСЫ

УДК 681.3

**С.Ф. Тюрин, В.С. Харченко**

Пермский государственный технический университет,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»,
(г. Харьков, Украина)

# ИЗБЫТОЧНЫЕ БАЗИСЫ ДЛЯ КРИТИЧЕСКИХ СИСТЕМ И ИНФРАСТРУКТУР ГОРОДСКОЙ СРЕДЫ: ОБЩИЙ ПОДХОД И ВАРИАНТЫ РЕАЛИЗАЦИИ

Развивается подход к созданию надежных и безопасных систем и инфраструктур городской среды, толерантных к отказам (различным негативным воздействиям), который основывается на использовании избыточных базисов. Сформулированы основные принципы автоматно-базисного подхода, позволяющего сохранить все функции или часть функций при отказах, и разработана автоматная модель. Описывается избыточный логический базис и даются рекомендации по его адаптации для инфраструктур городской среды.

**Ключевые слова:** критическая инфраструктура городской среды, избыточный базис, автоматная модель, функционально-полный толерантный базис, катастрофическое воздействие.

## Введение

***Актуальность. Проблема надежности систем и безопасность инфраструктур городской среды.*** Обеспечение функциональной безопасности информационно-управляющих систем (ИУС) критическими инфраструктурами, а также безопасности инфраструктур в целом является одной из ключевых проблем современной науки и инженерии. При этом речь идет о системах и инфраструктурах («системах систем») разной природы и разного назначения (системы управления атомными реакторами, аэрокосмическими комплексами, городскими инженерными коммуникациями и др.). В последнее

время на фоне возрастающих глобальных техногенных, климатических, террористических и других угроз значимость проблем безопасности городской среды многократно возросла.

Исторически сложилось так, что наиболее продуктивные идеи и решения появились в области цифровых вычислительных устройств и систем, хотя они носили и более общий характер. Ключевыми здесь были, по нашему мнению, работы J. Von Neumann [1], который сформулировал парадигму «надежных организмов из ненадежных компонент», A. Avižienis, который предложил принципы отказоустойчивости и N-версионного программирования [2], а затем (совместно с J.-C. Laprie, B. Randell, C. Landwehr) сформировал методологию гарантоспособных вычислений [3, 4].

Эволюция методов и технологий в сфере цифровых (и компьютерных) систем проанализирована в работе [5]. За последние десятилетия здесь наблюдалась нарастающая динамика роста терминов и парадигм, предложенных для создания надежных систем [6, 7]: устойчивых (fault-tolerant) и «эластичных» (fault-resilient) к отказам; естественно надежных (naturally reliable), естественно гарантоспособных (naturally dependable); отказобезопасных (fault-safe) и естественно безопасных (naturally safe); высокой готовности (high availability) и живучести (high syrvivability); самовосстанавливающихся (self-recovery) и «самоизлечивающихся» (self-healing) и др.

Для более сложных систем и инфраструктур, кроме того, получили развитие идеи, связанные с устойчивостью к катастрофам (disaster tolerance) и восстанавливаемостью при катастрофах (disaster recovery). Инфраструктурный контекст становится все более актуальным в связи с масштабностью инцидентов и аварий, происходящих вследствие естественных отказов, отказов и нарушений физической или информационной природы, которые носят непредумышленный или целенаправленный характер. Введен даже термин – критическая система инфраструктуры (КСИ). Все это обусловливает необходимость поиска не просто новых методов, а и новых парадигм с учетом специфики систем и среды, в которой они функционируют, учета взаимозависимости систем, образующих инфраструктуры, катастрофических воздействий, вызывающих отказы многих компонент и т.д.

***Постановка задачи.*** Большинство из известных методов обеспечения надежности систем основывается на применении различных видов избыточности, причем чаще всего эта избыточность применяется на канальном (системном) уровне, т.е. реализуется общее резервирование для системы в целом или ее наиболее важных подсистем. В то же время хорошо известно, что раздельное резервирование более эффективно. Кроме традиционных форм избыточности (резервирования) – аппаратной, информационной, временной, программной, теперь говорят и о территориальной, биологической, организационной и пр.

Что касается безопасности (далее речь идет о функциональной безопасности (safety)), то в рамках данной работы будем руководствоваться простым постулатом: пока система надежна (работоспособна), она безопасна. Это справедливо, если уровень, на котором должна обеспечиваться работоспособность, корректно обоснован и, если сформулированы и выполняются требования к уровню отказоустойчивости (например, требование, связанное с принципом единичного отказа [8]). В этом случае исключается ситуация, когда первый же отказ может стать критичным. Кроме того, здесь не рассматриваются методы, специфические для обеспечения безопасности (независимая верификация, диверсность и др. [9]).

Цель работы – разработка подхода, основанного на обеспечении надежности и безопасности на базисном уровне, т.е. базисной безопасности, основанной на сохранении после катастрофических воздействий некоторого базиса оставшихся функций, позволяющих восстановить часть функций, либо в самом крайнем случае – перевести систему в безопасное состояние.

Настоящая работа является развитием работы [10], в части автоматно-базисного подхода, и работ [11–14], где сформулированы принципы и реализованы методы синтеза систем на избыточных логических базисах.

## Автоматно-базисный подход к созданию надежных и безопасных систем

***Принципы автоматно-базисного подхода.*** Предлагаемый автоматно-базисный подход основывается на следующих принципах.

1. Концептуальным принципом является базисный подход к обеспечению надежности систем. Другими словами, обеспечение надежности осуществляется на уровне базисных компонент.

Такими базисами являются логический базис для микросхем (чипов с программируемой или фиксированной архитектурой), базис микросхем для цифровой или аналоговой системы, базис подсистем для инфраструктур.

2. Система (инфраструктура) строится с использованием компонент, обеспечивающих устойчивость (толерантность) к заданному набору и типам отказов или воздействиям, если известна модель воздействий, которая позволяет получить модель отказов или нарушений с требуемой детализацией. Под воздействием понимается явление любой природы (умышленное или непреднамеренное, случайное или детерминированное) и любого масштаба (одиночный сбой или отказ, множественный отказ в одной системе, катастрофический или кластерный отказ для инфраструктуры).

3. Компоненты, из которых строится система, имеют минимальную избыточность, чтобы обеспечить требуемую устойчивость к отказам. При этом должен обеспечиваться уровень устойчивости не ниже, чем при резервировании системы в целом.

4. Отказы, возникающие в одной компоненте, не могут влиять на работоспособность других компонент (снижать их устойчивость к отказам). При этом фактически обеспечивается принцип раздельного (покомпонентного) резервирования, поскольку отказы компонент не распространяются по системе или инфраструктуре.

***Автоматная модель системы, толерантной к воздействиям.*** Допустим, имеется система с некоторым множеством функций:

$$\Phi = \{\varphi_1, \varphi_2, ..., \varphi_n\}.$$

Пусть задана модель $\Psi$ воздействий в виде множества

$$\Psi = \{\Psi_1, \Psi_2, ..., \Psi_m\}.$$

Причем, в общем случае воздействие – некоторая цепочка (или множество цепочек) из $\Psi^*$, где $^*$ – итерация $\Psi$. В результате воздействия система деградирует, в частности, лишается некоторых функций:

$$\Phi^{\times} = \{\varphi_j^{\times i}\}, i = \overline{1,r}, j = \overline{1,k}, k \le n,$$

где $r$ – число вариантов деградации $j$-й функции; $k$ – число оставшихся функций, которые также могут деградировать.

Пусть требуется сохранить некоторое множество функций $\Phi^R \subset \Phi$ после воздействия. Тогда это можно описать композицией оставшихся функций или цепочками из $\Phi^{\times *}$, где $^*$ – соответствующая итерация. При этом могут дополнительно заданы временные $T_o$ и стоимостные ограничения $C_o$.

Функции системы представляются автоматными моделями, описывающими преобразование входных данных в выходные. Автоматная модель представляет собой пятерку [15]:

$$S = <X, Y, Z, \varphi, \psi>,$$

в которой $X = \{x_1, x_2,..., x_i\}$ – конечное входное множество (входной алфавит); $Y = \{y_1, y_2,..., y_j\}$ – конечное множество внутренних состояний автомата (алфавит состояний); $Z = \{z_1, z_2,..., z_k\}$ – конечное выходное множество (выходной алфавит); $\varphi$ – функция переходов (из состояния в другие состояния); $\psi$ – функция выходов; функция переходов представляет собой отображение вида $\varphi$: $X \times X \mapsto Y$; функция выходов представляет собой отображение вида $\psi$: $X \times Y \to Z$.

Таким образом, вместо абстрактных функций системы рассматривается множество автоматов $A = \{a_1, a_2, ..., a_n\}$, деградирующих в результате воздействий $\Psi^*$:

$$A^{\times} = \{a_j^{\times i}\}, i = \overline{1,r}, j = \overline{1,k}, k \le n.$$

Причем ставится условие обеспечения восстановления части автоматов $A^R \subset A$ после воздействия с заданными ограничениями $T_o, C_o$. В этом случае необходима суперпозиция автоматов, т.е. множество автоматов будет толерантным в случае, если после воздействий возможно указанное восстановление. Речь идет не о простом структурном резервировании, а о резервировании свойства базисности, т.е. о сохранении базиса, позволяющего восстановление.

Однако проблема функциональной полноты последовательностного автомата в общем случае алгоритмически неразрешима [16]. Тем не менее, любой автомат может быть представлен декомпозицией логического преобразователя и элементов памяти, а проблема функциональной полноты логического преобразователя разрешима в соответствии с теоремой Поста [17]. Логический

преобразователь – не что иное, как частный случай автомата – комбинационный автомат:

$$KS = <X, Z, \psi>.$$

Восстановление памяти автомата обеспечивается известными методами структурного резервирования и помехоустойчивого кодирования. Применительно к сложным системам она решается путем создания резервных хранилищ и коммуникаций. Таким образом, для $KS$ необходима не только функциональная полнота, но и ее сохранение после воздействий [18].

## Логический базис

***Сохранение базиса логического преобразователя при воздействии.*** В работах [11–14] разработана концепция избыточного логического базиса на вентильном уровне как альтернатива структурному резервированию. Он представляет собой функционально-полный толерантный базис (ФПТБ), сохраняющий при воздействии не саму исходную функцию, а функциональную полноту при заданной модели негативных воздействий (отказов). Один из вариантов функционально-полного толерантного базиса для модели константных однократных модификаций переменных имеет вид

$$\overline{x}_1\overline{x}_2 \vee \overline{x}_3\overline{x}_4$$

или

$$\overline{(x_1 \vee x_2)(x_3 \vee x_4)}.$$

Все модификации этой функции $f_{4383} = \overline{x}_1\overline{x}_2 \vee \overline{x}_3\overline{x}_4$: $\overline{x}_2 \vee \overline{x}_3\overline{x}_4$, $\overline{x}_1 \vee \overline{x}_3\overline{x}_4$, $\overline{x}_1\overline{x}_2 \vee \overline{x}_4$, $\overline{x}_3\overline{x}_4$, $\overline{x}_1\overline{x}_2$ представляют собой функции, обладающие функциональной полнотой в смысле теоремы Поста [16].

Представление в ФПТБ имеет вид

$$f = \bigvee_{i=1}^{r} \&_{j=1}^{S_i} x_i \to \overline{f}_{1.1}\overline{f}_{1.2} \vee \overline{f}_{2.1}\overline{f}_{2.2},$$

где $r$ – число конъюнкций в ДНФ; $S_i$ – число переменных в $i$-й конъюнкции. В свою очередь подфункции $f_{1.1}, f_{1.2}, f_{2.1}, f_{2.2}$ исходной функции могут быть представлены в виде

$$f_{ij} = \overline{f}_{ij.1.1}\overline{f}_{ij.1.2} \vee \overline{f}_{ij.2.1}\overline{f}_{ij.2.2},$$

и так далее, пока подфункции на определенном шаге не будут реализованы одним элементом.

Такое представление должно быть оптимальным по показателю количества операций вида $\overline{x}_1\overline{x}_2 \vee \overline{x}_3\overline{x}_4$.

Разработан метод, алгоритмы и программа автоматизированного синтеза в предлагаемом и остаточных базисах. Однако после воздействий функции этих ФПТ элементов изменяются, хотя и сохраняется функциональная полнота. Это усложняет процесс восстановления, поскольку необходимо установить, какие функции сохранились, после чего произвести реконфигурацию в соответствии с максимально возможным общим базисом. Если это невозможно, необходимо выбрать максимальное подмножество элементов, обладающих общим базисом.

***Сохранение функций логического преобразователя при воздействии.*** Сохранение исходных логических функций возможно методом так называемой учетверенной логики:

$$f = f_1 f_2 \vee f_3 f_4,$$

$$f_1 = f_2 = f_3 = f_4 = f.$$

При изменении любой одной из четырех функций функция системы не изменяется:

$$f = 1 f_2 \vee f_3 f_4 = f \vee ff = f, \; f_1 = 1.$$

$$f = 0 f_2 \vee f_3 f_4 = 0 \vee ff = f, \quad f_1 = 0.$$

$$f = \overline{f}_1 f_2 \vee f_3 f_4 = f\overline{f} \vee ff = 0 \vee ff = f, \; f_1 = \overline{f}_1.$$

В этом случае необходима четырехкратная избыточность, однако достаточно просто осуществляется объединение этих четырех функций – используется дизъюнкция. Для сохранения исходных функций возможно также использование трехкратной избыточности, но при этом применяется более сложная мажоритарная функция:

$$f = f_1 f_2 \vee f_1 f_3 \vee f_2 f_3, \; f_1 = f_2 = f_3 = f.$$

Например:

$$f = 1 f_2 \vee 1 f_3 \vee f_2 f_3 = f \vee f \vee ff = f, \quad f_1 = 1.$$

$$f = 0 f_2 \vee 0 f_3 \vee f_2 f_3 = 0 \vee 0 \vee ff = f, \quad f_1 = 0.$$

$$f = \overline{f}_1 f_2 \vee \overline{f}_1 f_3 \vee f_2 f_3 = 0 \vee 0 \vee ff = f, \quad f_1 = \overline{f}_1.$$

Можно показать, что мажоритирование базиса по сравнению со сложностью одного базисного элемента приводит на вентильном уровне к шести-, семикратной избыточности.

***Разработка модифицированного ФПТБ.*** Предлагается для сохранения базисной функции ИЛИ-НЕ $\overline{x}_1\overline{x}_2$ выражение

$$\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4 \vee \overline{x}_5\overline{x}_6\overline{x}_7\overline{x}_8.$$

Легко видеть, что в случае

$$\overline{x}_{1.1}\overline{x}_{2.1}\overline{x}_{1.2}\overline{x}_{2.2} \vee \overline{x}_{1.3}\overline{x}_{2.3}\overline{x}_{1.4}\overline{x}_{2.4}$$

функция ИЛИ-НЕ $\overline{x}_1\overline{x}_2$ сохранится при любой однократной константной модификации.

Например, при $x_{1.1} = 1$ «обнулится» левая конъюнкция и остается $\overline{x}_{1.3}\overline{x}_{2.3}\overline{x}_{1.4}\overline{x}_{2.4}$, что, очевидно, соответствует $\overline{x}_1\overline{x}_2$, поскольку переменные $x_{1.3} = x_{1.4} = x_1; \; x_{2.3} = x_{2.4} = x_2$.

При $x_{1.1} = 0$

$$\overline{x}_{2.1}\overline{x}_{1.2}\overline{x}_{2.2} \vee \overline{x}_{1.3}\overline{x}_{2.3}\overline{x}_{1.4}\overline{x}_{2.4},$$

что, очевидно, соответствует $\overline{x}_1\overline{x}_2$, поскольку переменные $x_{1.2} = x_{1.3} = x_{1.4} = x_1; \; x_{2.1} = x_{2.2} = x_{2.3} = x_{2.4} = x_2$.

Толерантность сохраняется и при инверсии переменной, например,

$$\overline{x}_{1.1} : \overline{\overline{x}}_{1.1}\overline{x}_{2.1}\overline{x}_{1.2}\overline{x}_{2.2} \vee \overline{x}_{1.3}\overline{x}_{2.3}\overline{x}_{1.4}\overline{x}_{2.4},$$

при этом аналогично $x_{1.1} = 1$ «обнулится» левая конъюнкция. Следовательно, обеспечивается парирование сбоев. Толерантность обеспечивается и при замыкании соседних линий связи, а также при некоторых кратных отказах.

Разработанный избыточный базис может быть использован как сложный (восьми переменных):

$$f = \overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4 \vee \overline{x}_5\overline{x}_6\overline{x}_7\overline{x}_8.$$

Например, может быть реализован частично резервированный ФПТ базис $\overline{x}_1\overline{x}_2 \vee \overline{x}_3\overline{x}_4$ в виде

$$f = \overline{x}_1\overline{x}_2\overline{x}_1\overline{x}_2 \vee \overline{x}_3\overline{x}_4\overline{x}_3\overline{x}_4.$$

Для сохранения базисной функции 2И-НЕ $\overline{x_1 \vee x_2}$ при модели однократных константных отказов может быть предложено выражение

$$\left(\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3 \vee \overline{x}_4\right)\left(\overline{x}_5 \vee \overline{x}_6 \vee \overline{x}_7 \vee \overline{x}_8\right),$$

т.е.

$$\left(\overline{x}_{1.1} \vee \overline{x}_{2.1} \vee \overline{x}_{1.2} \vee \overline{x}_{2.2}\right)\left(\overline{x}_{1.3} \vee \overline{x}_{2.3} \vee \overline{x}_{1.4} \vee \overline{x}_{2.4}\right).$$

Дальнейшим развитием подхода может быть сохранение более сложного и более эффективного ФПТ базиса $\overline{x}_1\overline{x}_2 \vee \overline{x}_3\overline{x}_4$ – для этого необходима функция

$$\left(\overline{x}_{1.1}\overline{x}_{2.1}\overline{x}_{1.2}\overline{x}_{2.2}\right)\left(\overline{x}_{1.3}\overline{x}_{2.3}\overline{x}_{1.4}\overline{x}_{2.4}\right) \vee \left(\overline{x}_{3.1}\overline{x}_{4.1}\overline{x}_{3.2}\overline{x}_{4.2}\right)\left(\overline{x}_{3.3}\overline{x}_{4.3}\overline{x}_{3.4}\overline{x}_{4.4}\right).$$

## Концепция расширения логического базиса для безопасных инфраструктур

Сложные объекты инфраструктур, как правило, слабо формализуются и в прямом виде, логические преобразования, описанные выше, вряд ли могут быть применены. В ряде случаев ограничиваются лишь графовыми моделями, описывающими отношения между объектами. Например, при анализе отказоустойчивости сетей (исследование и создание высоконадежных живучих управляющих информационных систем в ИПУ РАН [20]). Другой пример – переход от автоматных моделей к автоматно-непрерывным с целью анализа траекторий систем в критических ситуациях [21].

Тем не менее, в общем случае, не удается ограничиться лишь простейшей бинарной логикой. Однако это не означает, что базисный подход применим лишь на нижних уровнях инфраструктурной иерархии. Наметим три основных направления расширения базисного подхода. Первый – переход к модальным логикам, например, к многозначным логикам. Здесь исследователя также поджидает нерешенная до сих проблема функциональной полноты со всеми вытекающими последствиями. Но хорошо известны примеры функционально полных систем, на-

пример, система, включающая в себя константы и функции min, max, а также функции, использующие min, max и сложение по модулю. Возможен поиск толерантного базиса и в этой логике для соответствующей модели воздействий. Тогда получим $k$-значный толерантный базис.

Вторым направлением может быть использование нечетких множеств, нечеткой логики и нечетких алгоритмов, расширенной математическим аппаратом нечетких деградаций. Тогда необходим поиск таких нечетких моделей, которые при заданных нечетких деградациях либо сохраняли исходную модель, либо обеспечивали бы ее полное либо частичное заданное восстановление путем некоторых допустимых композиций (преобразований) деградированной модели. Здесь будет иметь место нечеткий толерантный базис.

Третье направление. Известно, для системы любой сложности может быть построена концептуальная (понятийная) модель, а иногда и реляционная. В этом случае появляется возможность перехода на новый уровень – на уровень логики предикатов, исчисления предикатов и реляционных алгебры и исчисления. Тогда некоторый объект инфраструктуры формализуется не просто булевым вектором, а вектором (или множеством векторов), элементы которых – некоторые $n$-местные предикаты (возможно не только первого порядка), описывающие исходные понятия и отношения:

$$\vec{V} : P_1, P_2, ..., P_i, ..., P_n.$$

В более сложном случае придется использовать не просто предикаты, а предикатные формулы $F$:

$$\vec{W} : F_1, F_2, ..., F_i, ..., F_n.$$

Размерность векторов, предикатов и формул зависит от степени детализации отказов компонент или иных учитываемых событий. Модель катастрофической ситуации может быть представлена модификациями такого вектора, например, формальной системой (системами) деградации. Должна быть найдена вторая формальная система – восстановления. Аксиомами ее будут выводы первой, а продукции должны обеспечить полное или частичное восстановление исходной модели. И это будет предикатная толерантность.

Наиболее общая постановка проблемы представляется авторам следующим образом.

Имеется две системы реальных объектов, процессов, явлений $C$ – защищаемая система и $K$ – угрожаемая система. Это необязательно технические системы, например, это могут быть и социальные, и биологические системы.

Вначале требуется получить математические объекты (модели) $\Phi_C$ и $\Psi_K$, описывающие системы $C$ и $K$.

Причем эти модели в наиболее важных для общества областях должны быть стандартизированы международным научно-техническим сообществом, а сама необходимость проектирования безопасной системы в конкретных областях – законодательно оформлена.

Задача анализа на этапе проектирования может заключаться в получении $\Phi_C^{\times}$ и определении, насколько эта модифицированная модель $\Phi_C^{\times}$ соответствует задаче проектирования безопасной системы и установленным ограничениям.

В случае несоответствия поставленным требованиям задача синтеза заключается в получении (поиске) модифицированной модели-2 (толерантно-базисной) $\Phi_C^2$, и ее преобразований $R$, таких, что $R(\Phi_C^{\times 2})$ удовлетворяет поставленным требованиям и ограничениям, а $\Phi_C^2$ является катастрофоустойчивой либо катастрофобезопасной.

Да, возможно, что в общем виде эти задачи не могут быть решены (скорее всего, окажутся алгоритмически неразрешимы), тогда надо будет искать частные случаи их решения, эвристики, использовать комбинаторный поиск на основе генетических и эволюционных вычислений. В конце концов, и природа не сразу нашла необходимые варианты и, возможно (мы на это надеемся), ищет что-то до сих пор, и будет искать еще долго.

## Заключение

В соответствии с базисным подходом к разработке надежных систем обеспечение надежности осуществляется на уровне базисных компонент. В данной работе этот подход развит для уровня избыточного логического базиса. Системы инфраструктур, которые строятся на основе избыточных базисов, могут быть названы естественно надежными, поскольку результаты

воздействий и отказов парируются на самом нижнем уровне – уровне компонент. Рассмотренные в работе функционально-полные толерантные базисы обеспечивают естественную в указанном смысле надежность таких систем.

При определенных условиях такие системы становятся и естественно безопасными, так как обеспечивается нечувствительность и к критичным отказам. Точнее говоря, критичные отказы не могут возникать или обычные отказы приводить к критичным.

В общем случае автоматно-базисный подход может быть применен для создания естественно надежных и безопасных инфраструктур. При этом возникает проблема выбора базиса и обеспечения его устойчивости к воздействиям заданного типа. Ее решение требует проведения дальнейших теоретических исследований и разработок. В частности, отдельной является проблема создания базисов, устойчивых к информационным воздействиям. Кроме того, интересным представляется исследование целесообразности использования многоверсионных технологий и соответствующих базисов для разработки гарантоспособных ИТ-инфраструктур [19].

Дальнейшим развитием подхода базисной безопасности может быть предлагаемая парадигма отказоустойчивого произвольного базиса. В этом случае возможно ставить в общем виде задачу синтеза естественно надежных систем произвольной функциональности. Представляется целесообразной ориентация на многозначные логики, в том числе нечеткую, на логику предикатов и формальные системы вообще.

## Библиографический список

1. J. Von Neumann. Probabilistic Logic and the Synthesis of Reliable Organisms from Unreliable Components / Automata Studies, C. Shannon and J. McCarthy (eds). Princeton University Press, 1956. – P. 43–98.

2. Avižienis A. Fault-Tolerance: The survival attribute of digital system // Proc. of the IEEE. – 1978. – Vol. 66, № 10. – P. 1109–1125.

3. Avižienis A., Laprie J.-C. Dependable Computing: From Concepts to Application // IEEE Trans. on Computers. – 1986. – № 74 (5). – P. 629–638.

4. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11–33.

5. Харченко В.С. Гарантоздатні системи та багатоверсійні обчислення: аспекти еволюції // Радіоелектронні і комп'ютерні системи. – 2009. – № 7.– С. 46–59.

6. TR 026764, ReSIST: Resilience for Survivability in IST. Deliverable D12 / Resilience-Building Technologies: State of Knowledge, September 2006. – 345 p.

7. Харченко В.С. Научно-методические результаты в области развития гарантоспособных систем // Радіоелектронні та комп'ютерні системи. – 2009. – № 4. – С. 24–33.

8. Yastrebenetsky M. A. (edit). Safety of Nuclear Power Plants: Instrumentation and Control Systems // Technika. – Kyiv, Ukraine, 2004 (NRC, 2007). – 472 p.

9. Айзенберг Я.Е., Ястребенецкий М.А. Сопоставление принципов обеспечения безопасности систем управления ракетоносителями и атомными электростанциями // Космічна наука та технологія. – 2002. – № 1. – С. 55–60.

10. Тюрин С.Ф., Харченко В.С. Автоматно-базисный подход к созданию естественно надежных и безопасных систем // Системи обробки інформації. – 2011. – № 1. – С. 55–60.

11. Тюрин С.Ф. Функционально-полные толерантные булевы функции // Наука и технология в России. – 1998. – № 4. – С. 7–10.

12. Тюрин С.Ф. Синтез адаптируемой к отказам цифровой аппаратуры с резервированием базисных функций // Приборостроение. – 1999. – № 1. – С. 36–39.

13. Тюрин С.Ф. Адаптация к отказам одновыходных схем на генераторах функций с функционально-полными толерантными элементами // Приборостроение. – 1999. – № 7. – С. 32–34.

14. Тюрин С.Ф. Проблема сохранения функциональной полноты булевых функций при «отказах» аргументов // Автоматика и телемеханика. – 1999. – № 9. – С. 176–186.

15. Горбатов В.А. Фундаментальные основы дискретной математики. Информационная математика: учеб. пособие для вузов. – М.: Наука, 2000. – 540 с.

16. Кузнецов О.П. Дискретная математика для инженера. – 3-е изд., перераб. и доп.— СПб.: Лань, 2004.— 395 с.

17. Марченков С.С. Замкнутые классы булевых функций. – М.: Физматлит, 2000. – С. 18.

18. Иыуду К. Надежность, контроль и диагностика вычислительных машин и систем. – М.: Высшая школа, 1989. – 219 с.

19. Kharchenko V.S. Multi-version Systems: Models, Reliability, Design Technologies, Proceeding of 10th ESREL Conference, Munich, Germany, 1999. – Vol. 1. – P. 73–77.

20. Каравай М.Ф. Инвариантно-групповой подход к исследованию *k*-отказоустойчивых структур // Автоматика и телемеханика. – 2000. – № 1. – С. 144–156.

21. Твердохлебов В.А. Геометрические образы поведения дискретных детерминированных систем // Радіо-електронні і комп'ютерні системи. – 2006. – № 5. – С. 161–165.

Получено 21.02.2011