УДК 621.3.019.3

А.В. ФЕДУХИН[*], П.Д. СЕСПЕДЕС ГАРСИЯ[*]

К ВОПРОСУ О СТРУКТУРАХ ОТКАЗОУСТОЙЧИВЫХ КОМПЬЮТЕРОВ ФИРМЫ STRATUS COMPUTER Inc.

[*]Институт проблем математических машин и систем НАН Украины, г. Киев, Украина

Анотація. *Стаття присвячена питанням інжинірингу відмовостійких комп'ютерів. Метою досліджень є аналіз технічних і програмних рішень, які використовуються при створенні сучасних відмовостійких комп'ютерів, а також розгляд можливості використання розробленої авторами квазімостікової структури як базової структури для створення відмовостійких комп'ютерів. Відомо, що основними способами забезпечення відмовостійкості засобів обчислювальної техніки є синтез електронних схем у вигляді d -безвідмовних комбінаційних схем і цифрових автоматів; резервування на рівні елементів функціональних складових частин і обчислювальних засобів е цілому. На сьогоднішній день методи синтезу безвідмовних цифрових автоматів обмежені розмірністю синтезованого об'єкта, вони дуже складні, вимагають великих обсягів обчислень і, як наслідок, не менш складних процедур щодо доведення досягнутого рівня відмовостійкості. Методи забезпечення відмовостійкості з використанням резервування більш прості і очевидні, тому що не вимагають додаткового підтвердження досягнутого рівня відмовостійкості. Цим і пояснюється їх широке застосування при створенні сучасних відмовостійких комп'ютерів і комп'ютерних систем. Тому важливим завданням інжинірингу є розробка методів і засобів комплексування вихідних нерезервованих складових частин у відмовостійкі комп'ютери, а саме розробка відмовостійких архітектур і структур технічних засобів та операційних систем і спеціального програмного забезпечення,що підтримують їх функціонування. Фірма Stratus Computer Inc. займає лідируюче положення на ринку відмовостійких технологій. Відмовостійкість комп'ютерів Stratus досягається за рахунок оригінальних архітектурних рішень і реалізації технології «Non-Stop», що забезпечує користувачеві безперервне функціонування комп'ютерної системи в цілому. Комп'ютери Stratus знаходять широке застосування в телекомунікаційних, банківських, біржових і багатьох інших додатках, а також як основа комп'ютерних систем відомих найбільших фірм.*

Ключові слова: *відмовостійкість, відмовостійкі комп'ютери, структурна схема, дублювання, активний сервіс, «гаряча» заміна.*

Аннотация. *Статья посвящена вопросам инжиниринга отказоустойчивых компьютеров. Целью исследований является анализ технических и программных решений, используемых при создании современных отказоустойчивых компьютеров, а также рассмотрение возможности использования разработанной авторами квазимостиковой структуры в качестве базовой структуры для создания отказоустойчивых компьютеров. Известно, что основными способами обеспечения отказоустойчивости средств вычислительной техники являются синтез электронных схем в виде d -безотказных комбинационных схем и цифровых автоматов; резервирование на уровне элементов функциональных составных частей и вычислительных средств в целом. На сегодняшний день методы синтеза безотказных цифровых автоматов ограничены размерностью синтезируемого объекта, они очень сложны, требуют больших объемов вычислений и, как следствие, не менее сложных процедур для доказательства достигнутого уровня отказоустойчивости. Методы обеспечения отказоустойчивости с использованием резервирования более просты и очевидны, так как не требуют дополнительного доказательства достигнутого уровня отказоустойчивости. Этим и объясняется их широкое применение при создании современных отказоустойчивых компьютеров и компьютерных систем. Поэтому важной задачей инжиниринга является разработка методов и средств комплексирования исходных нерезервированных составных частей в отказоустойчивые компьютеры, а именно разработка отказоустойчивых архитектур и структур тех-*

ISSN 1028-9763. Математичні машини і системи, 2018, № 4

нических средств и поддерживающих их функционирование операционных систем и специального программного обеспечения. Фирма Stratus Computer Inc. занимает лидирующее положение на рынке отказоустойчивых технологий. Отказоустойчивость компьютеров Stratus достигается за счет оригинальных архитектурных решений и реализации технологии «Non-Stop», обеспечивающей пользователю непрерывное функционирование компьютерной системы в целом. Компьютеры Stratus находят широкое применение в телекоммуникационных, банковских, биржевых и многих других приложениях, а также в качестве основы компьютерных систем известных крупнейших фирм.
Ключевые слова: *отказоустойчивость, отказоустойчивые компьютеры, структурная схема, дублирование, активный сервис, «горячая» замена.*

Abstract. *The article is devoted to the issues of engineering of fault-tolerant computers. The aim of the researches is to analyze the technical and software solutions used to create modern fault-tolerant computers, as well as to consider the possibility of using the quasi-bridge structure developed by the authors as the basic structure for creating fault-tolerant computers. It is known that the main ways of ensuring the fault tolerance of computer hardware are: synthesis of electronic circuits in the form of d -fault-free combinational circuits and digital automata; redundancy at the level of elements, functional components and computational tools in general. Nowadays, the methods of synthesis of reliable digital automata, unfortunately, are limited by the dimension of the synthesized object, they are very complex, require large amounts of calculations and, as a result, no less complex procedures for proving the achieved level of fault tolerance. Fault-tolerant methods with redundancy are simpler and more obvious, because they do not require additional proof of the achieved level of fault-tolerant. This explains their widespread use in the creation of modern fault-tolerant computers and computer systems. Therefore, an important task of engineering is the development of methods and means of integrating the original non-redundant components into fault-tolerant computers, namely the development of fault-tolerant architectures and hardware structures and operating systems supporting them and special software. Stratus Computer Inc.company occupies a leading position in the market of fault-tolerant technologies. Fault- tolerant of Stratus computers is achieved through original architectural solutions and the implementation of the "Non-Stop" technology, which ensures the user uninterrupted operation of the computer system as a whole. Stratus computers are widely used in telecommunications, banking, stock exchange and many other applications, as well as the basis of computer systems of well-known major companies.*
Keywords: *fault tolerance, fault-tolerant computers, block diagram, duplication, active service, hot standby.*

1. Введение

Отказоустойчивость является базовой платформой гарантоспособности компьютерных систем (КС) [1]. Известно, что основными способами обеспечения отказоустойчивости средств вычислительной техники являются синтез электронных схем в виде d-безотказных комбинационных схем и цифровых автоматов; резервирование на уровне элементов функциональных составных частей и вычислительных средств в целом. На сегодняшний день методы синтеза безотказных цифровых автоматов ограничены размерностью синтезируемого объекта, они очень сложны, требуют больших объемов вычислений и, как следствие, не менее сложных процедур для доказательства достигнутого уровня отказоустойчивости [2–5].

Методы обеспечения отказоустойчивости с использованием резервирования более просты и очевидны с точки зрения подтверждения достигнутого уровня отказоустойчивости. Этим и объясняется их широкое применение при создании современных отказоустойчивых компьютеров и компьютерных систем [6]. В данном контексте важной задачей инжиниринга является разработка методов и средств комплексирования исходных нерезервированных составных частей в отказоустойчивые компьютеры, то есть реализация известной парадигмы – «гарантоспособные системы из негарантоспособных составных частей».

Целью исследований является анализ технических и программных решений, используемых при создании современных отказоустойчивых компьютеров на фирме *Stratus Computer Inc.*, а также рассмотрение возможности использования разработанной авторами квазимостиковой структуры в качестве базовой структуры для создания отказоустойчивых компьютеров.

2. Отказоустойчивые компьютеры фирмы Stratus

Фирма Stratus [7] занимает лидирующее положение на рынке отказоустойчивых технологий. Отказоустойчивость компьютеров Stratus достигается за счет оригинальных архитектурных решений, а удобное их обслуживание со стороны пользователей является решающим фактором непрерывного функционирования КС в целом. Компьютеры Stratus находят широкое применение в телекоммуникационных, банковских, биржевых и многих других приложениях, а также в качестве основы КС известных крупнейших фирм.

В основе успеха продукции фирмы Stratus лежит технология, объединяющая в себе три фактора, обеспечивающие достаточно высокую отказоустойчивость КС:

• *Аппаратная отказоустойчивость с резервированием компонентов*

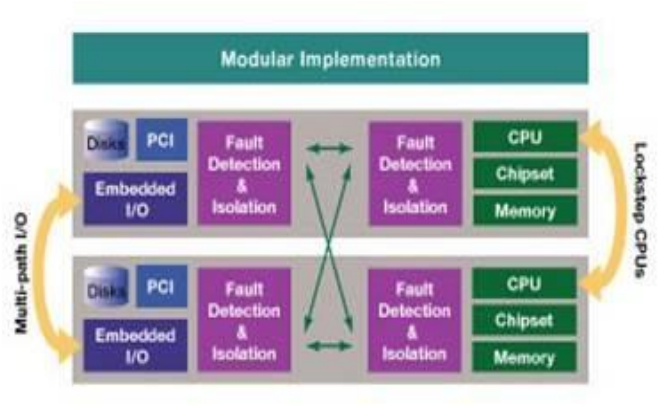

Рисунок 1 – Компоненты архитектуры Continuous Processing фирмы Stratus Computer Inc.

При этом используется жёсткая (потактовая) синхронизация процессов и данных в дублирующих друг друга компонентах. Все компоненты архитектуры Continuous Processing работают параллельно и согласованно для того, чтобы не просто минимизировать время незапланированного простоя, а совсем исключить его возникновение с высокой долей вероятности (рис. 1). Таким образом, в случае отказа одного из них не происходит потери данных и остановки компьютера в целом.

• *Программное обеспечение повышенной устойчивости*

В компьютере используются проверенные и/или улучшенные версии драйверов устройств, применяются политики, защищающие от случайной установки нестабильного/непроверенного программного обеспечения. Используются дополнительные средства для предотвращения сбоев, вызванных несовершенством программного кода приложений, а благодаря аппаратной архитектуре, исключаются программные сбои и сбои в микросхемах.

• *Архитектура активного сервиса*

Предусмотрена возможность «горячей» замены любого компонента (включая процессоры) без остановки приложений. После замены на исправные компоненты автоматически включаются в работу. Конструкция заменяемых блоков исключает ошибку при снятии/установке, поэтому замена может производиться пользователем самостоятельно. Компьютер автоматически извещает центр поддержки о происшествии или неисправности, после чего, при необходимости, нужный блок доставляется для замены. Замена компонента производится без прерывания обычной работы приложений.

3. Описание моделей компьютеров фирмы Stratus

Отказоустойчивость – специализация Stratus Computer Inc. (компании, сформированной в 1980 г.) – UNIX-серверы уровня предприятия семейства Stratus Continuum, спроектированные для критически важных применений, где цена простоя измеряется тысячами долларов в минуту и даже человеческими жизнями, и обеспечивают вероятность безотказной работы $R = 0{,}99999$ [8]. Машины Stratus обычно находят применение в крупных коммутируемых телекоммуникационных сетях, брокерских фирмах, банках, в электронной коммерции и обработке сообщений, здравоохранении, телефонных центрах службы спасения 911.

3.1. Семейство начального уровня Continuum 400

Ключевая характеристика машин Stratus – гарантированная двоичная совместимость с HP/UX, разновидности UNIX, разработанной компанией Hewlett-Packard. Машины Continuum Series 400 построены на базе RISC-микропроцессоров HP PA-7100, позже планируется выпустить серверы на базе более мощных ИС фирмы HP PA-8000.

Инженеры Stratus добиваются отказоустойчивости и непрерывной доступности ресурсов, применяя полное резервирование системы. Все внутренние компоненты машин Continuum дублированы, в том числе шина ввода-вывода, источники питания, накопители, центральный процессор (ЦП) и системная память. Среди прочих приемов, обеспечивающих отказоустойчивость и непрерывную доступность, «горячая» замена накопителей и источников питания; возможность вставлять платы PCI, ЦП и оперативного запоминающего устройства (ОЗУ), не отключая питания; операционная система, в которой предусмотрены меры по направлению потоков ввода-вывода в обход отказавших компонентов.

Компьютеры Continuum 400 состоят из двух «логических блоков», каждый со своей системной платой, ОЗУ, источником питания и спаренным ЦП. Все системные команды выполняются одновременно в обоих блоках, а результаты проверяются. Если обе половины функционируют одинаково, то обработка продолжается. Если же выявлено несовпадение, то исправная половина продолжает работу и в компанию Stratus автоматически отправляется сообщение об отказе блока, новый идентичный блок немедленно отправляется клиенту. Демонтаж отказавшего блока и установка присланного на замену агрегата могут быть произведены без отключения компьютера.

В целом в машине стоят четыре физических процессора, но они «дважды зарезервированы», в результате чего получается лишь один логический процессор. Процессоры выполняют все команды синхронно. Результаты, полученные каждым процессором, сверяются с результатами его дублера, а результаты пары – с результатами другой пары. В итоге все четыре процессора выполняют все команды и сравнивают результаты. Если хотя бы один из них отказал, то пара отключается и обработка продолжается до тех пор, пока неисправный блок не будет заменен. Время отказа и восстановления исключается из рабочего цикла, остается только непрерывная работа.

3.2. Промышленные компьютеры Stratus

В настоящее время компьютеры выпускаются под маркой Stratus ftServer. Они основаны на стандартных компьютерных архитектурах Intel, дополненных схемой выявления и изоляции отказов, поддерживающей непрерывную доступность системы, и оснащаются современными процессорами Intel Xeon.

Существует несколько семейств ftServer: стандартные W-series для промышленных предприятий, телекоммуникационные T-series и компьютеры V-series, поддерживающие VOS (virtual operating system), собственную операционную систему Stratus [7]. Все компьютеры фирмы Stratus рассчитаны на круглосуточную работу без остановки с обеспечением

минимального времени простоя и работы с показателем надёжности более $R = 0{,}99999$. Компьютеры используют технологию EM64T (Intel Extended Memory 64 Technology), обеспечивающую работу приложений, позволяющих быстро обрабатывать большие объёмы данных, располагать внушительные по размерам базы данных прямо в оперативной памяти, а также обращаться к неограниченному виртуальному адресному пространству.

Рассмотрим следующие промышленные отказоустойчивые (faultolerance) компьютеры, поддерживающие как 64-разрядную операционную систему Red Hat Enterprise Linux AS 4, так и ОС Windows Server (ftServer 2400, ftServer 2500, ftServer 4400, ftServer 6200).

Компьютер ftServer 2400

Это отказоустойчивый компьютер начального уровня с показателем надежности более $R = 0{,}99999$, представляющий третье поколение систем ftServer, пришёл на смену модели 2300. Область применения: типовые или повторяемые удаленные офисы, где предпочтительно полностью автоматизированное управление, компьютеризированные диспетчерские системы общественной безопасности небольших городов. «Горячая» замена компонентов: блок процессоров (1), блок ввода/вывода (1), диски (6). Операционные системы Windows Server 2003 Enterprise Edition и Red Hat Enterprise Linux4 (64-bit) 2003 Standart Edition.

Компьютер ftServer 2500

Новый двухъядерный высокодоступный компьютер Stratus ftServer 2500 на базе процессора Intel Xeon является младшей моделью в семействе отказоустойчивых систем четвертого поколения. Stratus ftServer 2500 более экономичен и прост в установке и обслуживании, чем отказоустойчивые кластеры. Поэтому он прекрасно подходит для поддержки работы критически важных приложений в удаленных офисах с ограниченной IT-поддержкой и высокими требованиями к отказоустойчивости. Stratus ftServer 2500 может использоваться в качестве отказоустойчивой альтернативы стандартному одиночному компьютеру. Преимущества: двухъядерный процессор Dual-core Intel Xeon, обеспечивающий высокую экономическую эффективность и производительность компьютера.

Компьютер ftServer 4400

Новый двухъядерный высокодоступный компьютер Stratus ftServer 4400 на базе одного или двух процессоров Intel Xeon относится к семейству отказоустойчивых систем нового поколения. Stratus ftServer 4400 подходит для поддержки отказоустойчивой работы критически важных приложений как в центрах обработки данных, так и в удаленных офисах, работающих без вмешательства человека. Например, Stratus ftServer 4400 может обеспечивать работу компьютеризированных диспетчерских центров общественной безопасности, производственных процессов. Преимущества**:** двухъядерные процессоры Dual-core Intel Xeon (система доступна в конфигурации с одним или двумя процессорами), обеспечивающие высокую производительность компьютера.

Компьютер ftServer 6200

Это самый производительный компьютер в семействе отказоустойчивых систем Stratus ftServer четвёртого поколения. Компьютер подходит для использования в крупных центрах обработки данных под информационные системы с интенсивным или непредсказуемо возрастающим потоком запросов, а также под системы консолидации информационной инфраструктуры на основе технологий виртуализации. Преимущества: использование новейшей компьютерной архитектуры и четырёхъядерных процессоров Intel Xeon; поддержка программных средств виртуализации VM Ware ESX.

Компьютеры ftServer 2500, ftServer 4400 и ftServer 6200 имеют модуль удалённого управления, который позволяет администраторам удаленно отслеживать работу системы;

Active Upgrade – технологию обновления программного обеспечения (ПО) на работающем без остановки компьютере, которая дает IT-специалистам возможность сократить время работ по регламентному обслуживанию; технологию Continuous Processing, обеспечивающую высочайший уровень бесперебойности без необходимости модифицировать приложения, писать программы, восстанавливающие систему после отказа, проводить тестирования и другие работы, как при подготовке приложений на кластерных системах.

Компьютеры выполнены в виде двух блоков, работающих параллельно и выполняющих одновременно одни и те же задачи. Эти блоки клиент может заменять в «горячем» режиме самостоятельно. Каждый из этих блоков эквивалентен стандартному компьютеру: содержит ЦП и устройства ввода-вывода. Для ОС и приложений два физических блока выглядят, как один логический компьютер. Если один из блоков выходит из строя, второй блок, ОС и приложение продолжают работать без каких-либо изменений. Таким образом, устраняется возможность непредвиденной остановки, обеспечиваются восстановление после отказа и вероятность потери данных. Подтвержденная практикой непрерывная готовность компьютеров Stratus превышает $K_{ОГ} = 0{,}99999$. «Горячая» замена компонентов – блок процессоров (1 или 2), блок ввода/вывода (1), диски (6). Операционные системы Windows Server 2003 Enterprise Edition и Red Hat Enterprise Linux4 (64-bit) 2003 Standart Edition.

Сервер RADIO Cluster PC

Ни для кого не секрет, что повседневная деятельность компаний сегодня попадает во все большую зависимость от Internet [9]. Учитывая это, фирма Stratus Computer выпустила отказоустойчивую платформу для сервера Windows NT Server под названием RADIO Cluster PC. Ее главное предназначение – обеспечить непрерывную и безотказную работу особо важных приложений Сети и баз данных SQL. Аббревиатура RADIO расшифровывается как Reliable Architecture Distributed I/O (архитектура повышенной надежности с распределенным вводом-выводом).

Предлагаемая платформа делает сервер доступным постоянно, его работа не прерывается даже на время установки нового ПО, корпус сервера RADIO Cluster PC открывает удобный доступ к компонентам и обеспечивает их легкую «горячую» замену. Чтобы добиться максимальной надежности, Stratus прибегла к резервированию всех элементов своей платформы. Используя стандартные аппаратные средства ПК, разработчики RADIO Cluster PC провели дублирование таких функциональных подсистем своего устройства, как процессорный узел, блоки хранения информации и подключения к сети. Координация работы всех компонентов платформы осуществляется специализированным ПО кластеризации.

В RADIO Cluster PC воплощена современная комплексная технология, которая отлично справляется с поставленными задачами. Например, все входящие в него элементы снабжены собственными административными консолями. Конструкция RADIO Cluster PC весьма своеобразна. Все компоненты устройства изготовлены в виде блоков «горячей» замены, так называемых «центров» (node), вставляемых в восемь отсеков корпуса.

Выполнение основных серверных функций осуществляется в вычислительном центре Compute Node. В центре хранения Storage Node, назначение которого ясно из его названия, предусмотрено место для установки четырех накопителей с интерфейсом Fast/Wide SCSI. Внутренние концентраторы системы размещены в сетевых центрах Network Node. Все центры устанавливаются в общий корпус попарно, что обеспечивает полное их дублирование. Для соединения центров между собой в корпусе проложены две независимые сети на базе передающей среды Fast Ethernet и витой пары 10 BaseT. Первая соединяет вычислительные центры с центрами хранения, обеспечивая скорость обмена данными 100 Мбит/с. Она же используется для подключения к корпоративной магистрали.

Каналы 10BaseT служат для внутреннего управления системой, главным образом для передачи сигнала синхронизации между узлами и выполнения операций администрирования RADIO Cluster PC. Каналы с пропускной способностью 10 Мбит/с обеспечили хорошее качество управления всеми вычислительными центрами RADIO Cluster PC. Процедуры управления функционально сходны с работой за обычной консолью.

Чтобы производить конфигурирование и мониторинг работы вычислительных центров, необходимо подключиться к вспомогательной сети и воспользоваться пакетом PCAnywhere for Windows корпорации Symantec, фактически уже превратившимся в стандартное приложение дистанционного управления.

Новый продукт снабжен ПО кластеризации под названием IAM (Isis Reliable and Active Replication – надежная активная репликация Isis). Определение сбоев в работе приложений и устранение их последствий осуществляется на основе комплекса правил и тесной связи программы с этими приложениями.

При выходе из строя центра А работающее на нем приложение переводится на центр В. Высокое быстродействие достигается за счет использования виртуального, а не физического IP-адреса. Для клиента подобный процесс выглядит обычной для сети задержкой в получении данных и не вызывает никаких последствий. Продукт Stratus является полноценным кластером, поэтому обратный перевод центра в рабочее состояние не требует повторного переключения блоков. Такая прозрачность в работе системы – непременное условие обеспечения ее полной отказоустойчивости.

Свой новый продукт фирма Stratus оснастила сценариями восстановления работоспособности SQL Server, Exchange и IIS корпорации Microsoft. Также в комплект RADIO Cluster PC включен инструментарий разработчика, позволяющий произвести настройку кластера для работы с ними. Использование сценариев Perl дает возможность создавать специализированные процедуры контроля, следящие за функционированием серверов и устраняющие сбои в их работе. Вычислительные центры Compute Node представляют собой файловые серверы, работающие под управлением Windows NT. Каждый из них оснащен двумя процессорами Pentium и загрузочным жестким диском.

4. Классификация двухканальных резервированных структур

Итак, основными структурами, обеспечивающими отказоустойчивость компьютеров фирмы Stratus Computer Inc., являются дублированные структуры. Причем дублирование осуществляется на уровне функциональных блоков различной элементоемкости и уровня надежности. В связи с тем, что ноу-хау реализации комплексирования структур по понятным причинам не разглашаются, то приведем краткую классификацию различных реализаций дублированных структур и сформулируем их основные достоинства и недостатки [10].

4.1. Дублированная система со слабыми связями

Примечание. В качестве обозначенных на рис. 2 ЭВМ 1,2 могут быть как компьютеры в целом, так и любые другие их составные части и функциональные блоки: процессоры, шины данных, устройства ввода-вывода, дисковые накопители данных, источники питания и т.д.

Дублированная система со слабыми связями состоит из двух вычислительных каналов, в которых процессоры и программы могут быть различными. Процессор ЭВМ1 реализует основные вычисления, а ЭВМ2 их проверяет. Для этого осуществляется обмен информацией по шине W . Синхронизация каналов не обязательна.

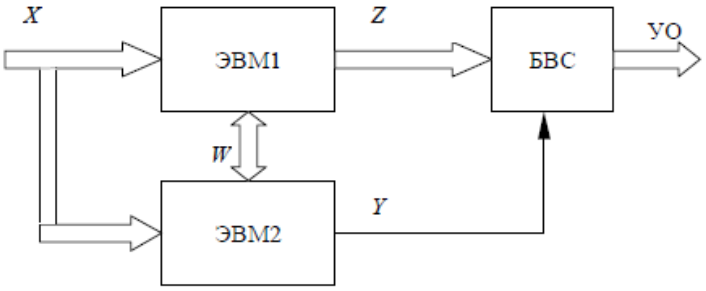

Рисунок 2 – Дублированная система со слабыми связями

Отказоустойчивость таких систем зависит от достоверности контроля функционирования вычислительных каналов. Контроль работы ЭВМ осуществляется либо за счет тестовых программ, либо за счет параллельных вычислений одинаковыми или диверситетными программами и сравнения результатов. При обнаружении ошибки ЭВМ2 формирует сигнал ***Y*** и выходы ЭВМ1 отключаются от управляемых объектов (УО) или информационных выходов (ИВ) с помощью безопасных выходных схем (БВС).

При организации параллельных вычислений по одинаковым алгоритмам возможно сравнение промежуточных результатов вычислений в контрольных точках. Сравнение результатов производится программно в ЭВМ2. Для обеспечения своевременного отключения отказавшего вычислительного канала необходимо, чтобы контролирующая ЭВМ выполняла вычисления не медленнее, чем основная ЭВМ. Это достигается либо использованием процессора с более высоким быстродействием, либо использованием программ с более короткими алгоритмами вычислений. При этом необходимо обеспечить одновременное считывание исходных данных в оба вычислительных канала. Возможно использование и идентичных вычислительных каналов, и программного обеспечения.

Достоинства: высокая гибкость; возможность использования диверситетных вычислительных каналов, что позволяет с высокой точностью обнаруживать отказы аппаратных средств и ошибки при проектировании программного обеспечения; отсутствие синхронизации каналов, что упрощает схемную реализацию и уменьшает вероятность возникновения одинаковых отказов и сбоев в обоих каналах.

Недостатки: высокие затраты на проектирование диверситетных вычислительных каналов и программного обеспечения; сложность выбора точек для контроля промежуточных вычислений, так как требуется обеспечить высокую достоверность контроля при минимальном количестве проверок; возможность накопления маскируемых отказов в обоих вычислительных каналах; необходимость организации контроля за правильностью программного сравнения результатов в ЭВМ2, так как отказы в ЭВМ2 не должны искажать результаты контроля; невысокая эксплуатационная готовность, так как любой отказ переводит систему в нерабочее защитное состояние.

4.2. Дублированная система с умеренными связями

Дублированная система с умеренными связями включает в себя два одинаковых вычислительных канала с одинаковыми программами. Это одна из наиболее распространенных на практике отказоустойчивых структур.

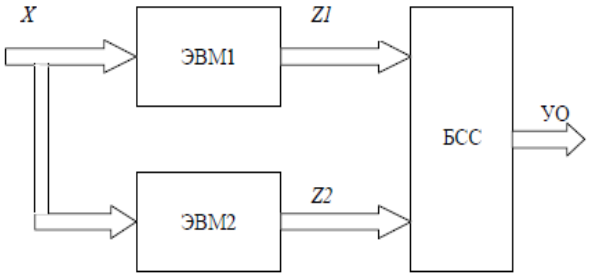

Рисунок 3 – Дублированная система с умеренными связями

Работа обоих каналов синхронизирована. Синхронизация служит для одновременного считывания входных воздействий ***X*** и одновременной выдачи результатов ***Z1*** и ***Z2***. Необходимость синхронизации обусловлена циклической непрерывной работой системы, когда даже при одинаковых технических средствах и одинаковых программах из-за разброса временных параметров со временем может

произойти рассогласование работы каналов.

Результаты обработки информации сравниваются на уровне выходов ***Z1*** и ***Z2*** с помощью безопасной схемы сравнения (БСС). При обнаружении рассогласования работы каналов БСС переводит свои выходы в защитное состояние и блокируется. Минимальная кратность необнаруживаемых отказов в системе равна двум – по одному отказу в каждом вычислительном канале, которые одинаковым образом искажают выходные сигналы ***Z1*** и ***Z2***.

Одиночные отказы не опасны, если они искажают выходные сигналы и обнаруживаются БСС. В противном случае возможно накопление отказов. Для исключения накопления отказов вычислительные каналы снабжаются средствами самотестирования, то есть реализуется временная избыточность. Тесты разрабатываются таким образом, чтобы любой отказ аппаратных средств на одной из тестовых последовательностей исказил значения выходных сигналов. Кратные независимые отказы должны обнаруживаться БСС.

Достоинства: простота реализации; невысокая стоимость; высокая отказоустойчивость.

Недостатки: возможность накопления маскируемых отказов в обоих вычислительных каналах; невозможность обнаружения ошибок проектирования в программном обеспечении, так как они одинаково проявляются в обоих каналах; невысокая эксплуатационная готовность, так как любой отказ переводит систему в нерабочее защитное состояние. Применяется там, где не предъявляются высокие требования к эксплуатационной готовности.

4.3. Дублированная система с сильными связями

Дублированная система с сильными связями использует одинаковые программы в двух одинаковых вычислительных каналах, но в отличие от системы с умеренными связями контроль работы двух каналов осуществляется не только на уровне выходов, но и на уровне шин передачи данных и памяти.

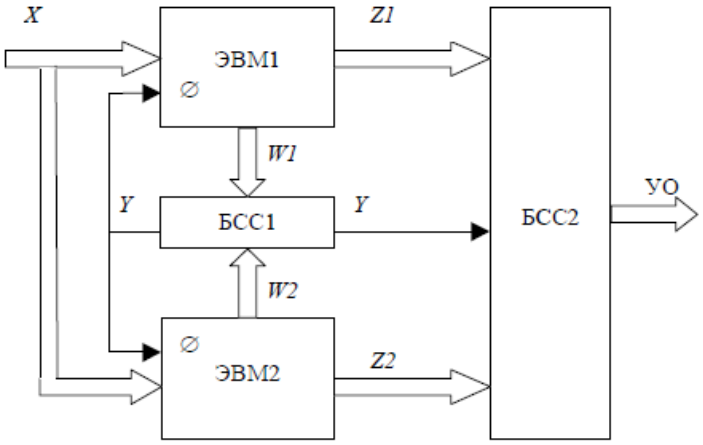

Рисунок 4 – Дублированная система с сильными связями

Работа каналов синхронизирована. Синхронизация организуется либо по командам, либо по тактам. В наиболее сильном случае производится потактовая проверка совпадения сигналов ***W1*** и ***W2*** на внутренних контрольных точках (шинах) с помощью БСС1. При расхождении сигналов ***W1*** и ***W2*** БСС1 формирует сигнал ошибки ***Y***. Сигнал ***Y*** воздействует на БСС2 и отключает УО, то есть переводит оба канала в защитное состояние. Затем сигнал ***Y***, поступая на вход ***Ø***, блокирует работу двух ЭВМ.

Структура обладает высоким уровнем отказоустойчивости, который зависит от вида и числа контролируемых разрядов (сигналы ***W1*** и ***W2***). Одиночные отказы неопасны и должны обнаруживаться БСС1. Однако, если множество входных воздействий ***X*** не обеспечивает необходимой глубины проверки каналов обработки информации, то возможно появление маскируемых отказов, то есть отказов, которые не проявляются на данном промежутке времени в виде расхождения сигналов ***W1*** и ***W2***. Накопление таких отказов может

привести к опасному отказу системы. Это тем более актуально, что некоторые алгоритмы функционирования системы могут выполняться очень редко (раз в неделю или раз в месяц).

Достоинства: невысокая стоимость; затраты на проектирование вычислительных каналов и программного обеспечения ниже, чем в других структурах; высокая глубина контроля отдельных функциональных узлов ЭВМ (процессора, памяти, портов ввода-вывода).

Недостатки: возможность накопления маскируемых отказов в редко используемых функциональных узлах вычислительных каналов; невозможность обнаружения ошибок проектирования в программном обеспечении, так как они одинаково проявляются в обоих каналах; необходимость обеспечения высокой надежности схемы синхронизации каналов; невысокая эксплуатационная готовность, так как любой отказ переводит систему в нерабочее защитное состояние.

4.4. Самопроверяемая дублированная система

Самопроверяемая дублированная система состоит из двух каналов, построенных в виде самопроверяемых устройств. Каждый вычислительный канал снабжается самопроверяемой схемой внутреннего контроля (ССВК), задачей которой является обнаружение неисправностей заданного класса в вычислительном канале и собственных неисправностей. Самопроверяемые схемы внутреннего контроля каждого канала при обнаружении ошибки вырабатывают сигнал ***Y***, который отключает соответствующий вычислительный канал.

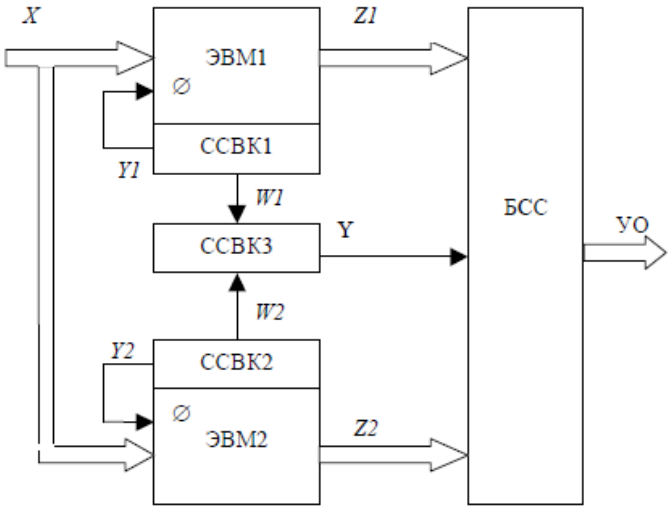

Рисунок 5 – Самопроверяемая дублированная система

Выходные сигналы ***Z1*** и ***Z2*** сравниваются БСС. При совпадении сигналов формируется управляющее воздействие на УО. Сигналы контроля ***W1*** и ***W2***, формируемые с помощью ССВК1 и ССВК2, сравниваются в ССВК3. При обнаружении ошибки ССВК3 вырабатывает сигнал ***Y***, который переводит безопасную схему сравнения в защитное состояние.

Самоконтроль каналов может быть аппаратный и программный. Возможно использование независимых (диверситетных) программ в каждом процессоре.

Достоинства: высокая глубина контроля вычислительных каналов; высокая отказоустойчивость; возможность выделения отказавшего вычислительного канала.

Недостатки: сложность определения критериев правильной работы системы для реализации ССВК; невозможность обнаружения ошибок в программном обеспечении при использовании одинаковых программ; сложность реализации системы, особенно при использовании диверситетных вычислительных каналов; невысокая эксплуатационная готовность, так как любой отказ переводит систему в нерабочее защитное состояние.

Выводы по результатам анализа дублированных структур

Отличием представленных дублированных структур (рис. 3–5), имеющих выходную схему с логической функцией «И» (БСС), которые могут использоваться в компьютерах Stratus, является то, что для реализации режима «горячей» замены отказавшей состав-

ной части компьютеров выходная схема дублированной структуры должна выполнять логическую функцию «И/ИЛИ». Поэтому такой общий недостаток в виде низкой эксплуатационной готовности, присущий всем приведенным выше схемам дублирования с выходной функцией восстанавливающего органа (ВО) в виде «И», в реальных компьютерах Stratus отсутствует.

Один из вариантов синтеза ВО с переменной логической функцией «И/ИЛИ», реализованный в виде самопроверяемой дублированной системы с квазимостиковой структурой, приведен на рис. 6.

4.5. Самопроверяемая дублированная система с квазимостиковой структурой

С целью повышения эксплуатационной готовности самопроверяемой дублированной системы был разработан новый класс самопроверяемой дублированной системы с квазимостиковой структурой (СДКМС) [11–16].

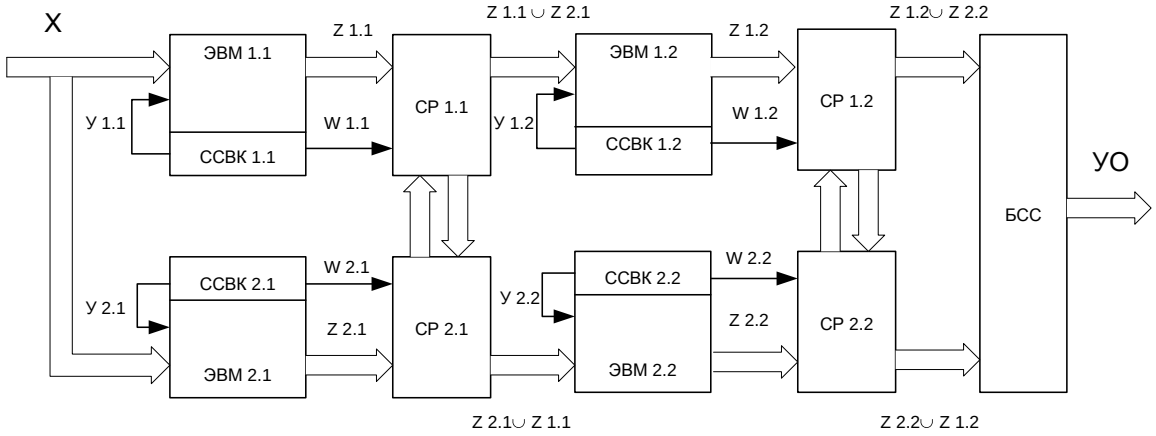

Рисунок 6 – Самопроверяемая дублированная система с квазимостиковой структурой

Повышение отказоустойчивости и эксплуатационной готовности самопроверяемой дублированной системы (рис. 5) достигается декомпозицией (дихотомией – последовательным делением целого на две части, затем каждой из них снова на две части и т.д.), при которой каждый вычислительный канал (ЭВМ) разбивается на *n* равнонадежных элементов структуры (функциональных блоков ФБ), которые с помощью схем реконфигурации (СР), имеющих логическую функцию «И/ИЛИ», образуют *n* дублированных равнонадежных узлов. Анализ работоспособности каналов осуществляется парой ССВК, а выходной контроль работоспособности всей структуры осуществляется БСС с логической функцией «И».

Примечание. Разбиение вычислительного канала на равнонадежные или приблизительно равнонадежные ФБ приводит к наибольшему эффекту – возрастанию вероятности безотказной работы и эксплуатационной готовности системы.

Схема декомпонированной структуры, состоящей из двух узлов, приведена на рис. 6. Визуально она напоминает мостиковую структуру, в которой вместо центрального типового элемента структуры установлены две СР (по одной в каждый канал), которые обеспечивают перекрестные связи между каналами с целью реконфигурации структуры в случае выхода из строя соответствующего ФБ канала.

В нормальном режиме пара СР реализует логическую функцию «**И**» (осуществляется непрерывный контроль синхронности работы каналов), в случае отказа одного из ФБ канала (появление сигнала от аппаратных и/или программных средств внутреннего контроля ССВК), СР изменяет свою логическую функцию на «**ИЛИ**» и осуществляет беспре-

пятственное прохождение информации с выхода исправного ФБ узла к следующему узлу, распараллеливая ее на два канала. В таком состоянии система находится до момента восстановления работоспособности отказавшего ФБ либо в автоматическом режиме (за счет самодиагностики и самовосстановления), либо в результате осуществления режима «горячей» замены со стороны оператора. Для достижения отказоустойчивости системы в целом обеспечиваются функциональная автономность и независимость каждого ФБ от других компонентов системы, чтобы при выходе из строя любого ФБ последний не оказывал негативного влияния на работу других ФБ и всей системы в целом.

Достоинства: с ростом количества узлов растет эксплуатационная готовность системы; уменьшается сложность ФБ, из которых состоит узел, что упрощает программную и/или техническую реализацию ССВК, повышает точность контроля и диагностики неисправностей структуры и, как следствие, приводит к уменьшению времени восстановления и возрастанию показателей надежности восстанавливаемой квазимостиковой структуры в целом. Обнаруженный положительный эффект от разбиения системы на равнонадежные дублированные узлы и использование реконфигурации структуры в случае отказа ФБ позволяют более эффективно осуществлять структурный синтез высоконадежных отказоустойчивых компьютеров и КС.

Недостатки: необходимость в дополнительных технических средствах для реализации СР, ССВК и БСС.

5. Пример аппаратной реализации самопроверяемой дублированной системы с квазимостиковой структурой

На аппаратном уровне принцип построения системы можно проиллюстрировать следующим образом. Вокруг каждого выхода ФБ организуется структура обнаружения неисправностей и генерации управляющих сигналов на схему реконфигурации системы (рис. 7).

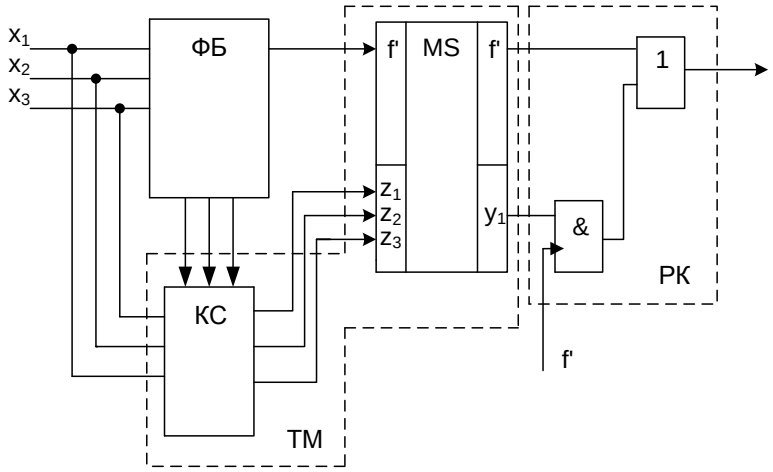

Рисунок 7 – Аппаратная реализация тестора-мультиплексора (ТМ) и реконфигуратора (РК)

Такая структура работает следующим образом. В ФБ происходит обработка входных воздействий X_1,X_2,X_3. Правильность функционирования ФБ проверяется контрольной схемой (КС). КС с функцией ССВК (рис. 6) может быть построена на высокочастотной ПЛИС или реализована программным путем. КС через мультиплексор (MS) формирует управляющий сигнал для реконфигуратора (РК). В зависимости от вида такого сигнала 0/1 РК пропускает выходной сигнал с ФБ далее или блокирует его, одновременно принимая сигнал с другого исправного ФБ.

В общем виде иллюстрация аппаратной реализации двухканальной структуры с реконфигурацией, состоящей из двух узлов, выглядит следующим образом (рис. 8).

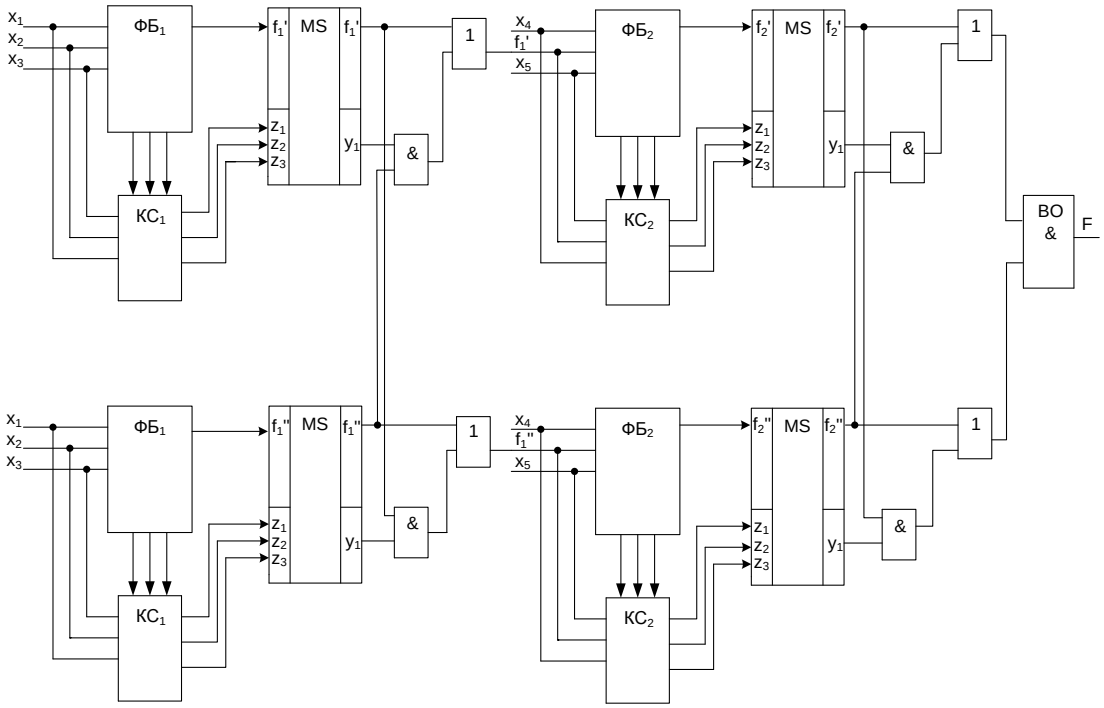

Рисунок 8 – Пример аппаратной реализации двухканальной структуры с реконфигурацией

6. Выводы

Квазимостиковая структура характеризуется более высоким уровнем отказоустойчивости и, как следствие, эксплуатационной готовности, так как имеет значительно большее количество работоспособных состояний, чем простая дублированная структура. Она способна к автоматической реконфигурации в одноканальную структуру без дополнительного вмешательства и изменения функции восстанавливающего органа (ВО).

Исследованиями также установлено, что средняя наработка до отказа СДКМС интенсивно возрастает с уменьшением времени восстановления и имеет тенденцию к увеличению с ростом количества узлов при фиксированном времени восстановления.

Вероятность безотказной работы СДКМС также возрастает с уменьшением времени восстановления и возрастает при увеличении количества узлов, а коэффициент вариации наработки до отказа СДКМС снижается с уменьшением времени восстановления и ростом количества узлов.

При увеличении количества узлов тенденция уменьшения коэффициента вариации наработки до отказа является дополнительным фактором, влияющим на рост вероятности безотказной работы восстанавливаемой СДКМС. Кроме того, с ростом количества узлов уменьшается сложность ФБ, из которых состоит узел, что упрощает программную и/или техническую реализацию ССВК, повышает точность контроля и диагностики неисправностей структуры и, как следствие, приводит к уменьшению времени восстановления и возрастанию показателей надежности восстанавливаемой СДКМС в целом.

Обнаруженные положительные эффекты от разбиения структуры на равнонадежные дублированные узлы (дихотомии) и использование реконфигурации структуры в случае отказа составных частей позволяют разработчикам проектировать на ее основе более эффективные отказоустойчивые компьютеры и КС.

СПИСОК ИСТОЧНИКОВ

1. Федухин А.В., Сеспедес Гарсия Н.В. Атрибуты и метрики гарантоспособных компьютерных систем. *Математичні машини і системи*. 2013. № 2. С. 195–201.
2. Сапожников В.В., Кравцов Ю.А., Сапожников Вл.В. Дискретные устройства железнодорожной автоматики, телемеханики и связи. М.: Транспорт, 1988. 255 с.
3. Сапожников В.В., Сапожников Вл.В., Христов Х.Л., Гавзов Д.В. Методы построения безопасных микроэлектронных систем железнодорожной автоматики. М.: Транспорт, 1995. 272 с.
4. Сапожников В.В., Сапожников Вл.В. Дискретные автоматы с обнаружением отказов. Л.: Энергоатомиздат, 1984. 109 с.
5. Сапожников В.В., Сапожников Вл.В. Самопроверяемые дискретные устройства. СПб.: Энергоатомиздат, 1992. 224 с.
6. Станчак М. Дублирование – залог надежности. URL: https://www.itweek.ru/infrastructure/article/detail.php?ID=76505.
7. Отказоустойчивые компьютеры ведущих фирм для построения отказоустойчивых систем. Stratus Computer Inc. Мальборо, Массачусетс, (508) 460-2000. URL: http://www.stratus.com.
8. UNIX-серверы Continuum обеспечивают непрерывную доступность ресурсов Stratus Continuum Series 400 Stratus Computer Inc. Мальборо, Массачусетс, (508) 460-2000. URL: http://www.stratus.com.
9. Станчак М. Stratus гарантирует высокую отказоустойчивость (084)10`1997 ОБЗОР RADIO Cluster PC предотвращает простои BackOffice. URL: http://www.citforum.idknet.com/hardware/articles/stratus00.shtml.
10. РТМ 32 ЦШ 1115842.01-94. Безопасность железнодорожной автоматики и телемеханики. Методы и принципы обеспечения безопасности микроэлектронных СЖАТ. СПб.: ПГУ ПС, 1994. 120 с.
11. Федухин А.В., Муха Ар.А. К вопросу об аппаратной реализации избыточных структур: резервированная двухканальная система с реконфигурацией. *Математичні машини і системи*. 2010. № 4. С. 156–159.
12. Федухин А.В., Муха Ар.А. Имитационное моделирование отказоустойчивой резервированной двухканальной системы в интегрированной инструментальной среде Matlab Simulink. *Математичні машини і системи*. 2011. № 2. С. 178–181.
13. Федухин А.В., Пасько В.П. Моделирование надежности восстанавливаемой квазимостиковой структуры с учетом тренда параметров надежности составных частей. *Математичні машини і системи*. 2014. № 3. С. 125–135.
14. Федухин А.В., Пасько В.П. К вопросу о моделировании надежности двухканального невосстанавливаемого вычислительного комплекса специального назначения. *Математичні машини і системи*. 2016. № 4. С. 142–145.
15. Федухин А.В., Пасько В.П., Муха Ар.А. К вопросу моделирования надежности восстанавливаемой квазимостиковой структуры с учетом тренда параметров надежности составных частей // *Математичні машини і системи*. 2016. № 1. С. 158–167.
16. Федухин А.В., Сеспедес Гарсия Н.В., Муха Ар.А. К вопросу о надежности невосстанавливаемой системы с квазимостиковой структурой элементов. *Математичні машини і системи*. 2017. № 4. С. 160–168.

Стаття надійшла до редакції 16.11.2018