И.Б. Шубинский

«НАДЕЖНЫЕ ОТКАЗОУСТОЙЧИВЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»

Предлагаемая читателю книга «Надежные отказоустойчивые информационные системы. Методы синтеза» является третьей заключительной частью проекта «Надежность информационных систем».

Основные идеи построения надежных и безопасных информационных систем изложены в первой главе «Основы надежности и отказоустойчивости информационных систем». Эта глава предназначена для лиц принимающих решения, которым достаточно понимать проблему на концептуальном уровне. В этой главе изложены постулаты обеспечения надежности информационных систем, ключевые понятия избыточности, отказоустойчивости, отказобезопасности и киберзащищенности систем.

Во второй главе книги развиты традиционные модели надежности как невосстанавливаемых, так и восстанавливаемых объектов с общим и раздельным постоянным резервированием, а также резервированием замещением в целях учета скрытых отказов и учета реальных возможностей средств их обнаружения. Особый интерес представляют модели надежности объектов с мажоритарным резервированием, в которых совмещены модель структурной надежности мажоритарного объекта и функциональной надежности его восстанавливающего органа. В главе выполнена предельная оценка надежности резервированных объектов с бесконечным количеством резервных устройств, но ограниченной эффективностью системы обнаружения отказов, которая убедительно показывает, что не следует питать иллюзии относительно достижения требуемого уровня надежности системы за счет увеличения количества резервных устройств. Скромные возможности структурного резервирования, как с восстановлением, так, и тем более, без восстановления, вызывают необходимость в разработке нетривиальных методов обеспечения отказоустойчивости информационных систем. Это тем более важно, что рассчитывать на эффективное применение временного и/или функционального резервирования в информационно – управляющих системах, работающих в реальном времени, не представляется возможным. В главе также систематизированы методы информационного резервирования, основанные на различных требованиях к эффективности контроля достоверности хранимой информации.

В третьей главе представлены оригинальные методы построения модульных информационных систем с адаптивной отказоустойчивостью. Изложены идеи адаптивной отказоустойчивости (активной защиты), приведены способы организации активной защиты, способы автоматического обнаружения и устранения неисправностей, временные интервалы и дисциплины активной защиты. Оценена эффективность применения методов активной защиты. Изложен метод синтеза активной защиты. Показаны несомненные преимущества активной защиты перед традиционными методами структурного резервирования как в отношении надежности, так и в отношении технико – экономических показателей. При этом активная защита обеспечивает возможности адаптации системы не только к отказам, но и к сбойным и программным ошибкам.

В четвертой главе описаны методы построения надежных программных средств, в том числе обсуждены их характерные недостатки, приведены рекомендации по разработке спецификации требований к проектируемым программам, достаточно подробно раскрыта технология разработки архитектуры надежной программы. Большое внимание уделено вопросам проектирования надежного программного обеспечения и его реализации, в том числе верификации программ и их интеграции с аппаратными средствами, а также их аттестации, эксплуатации, сопровождению и конфигурации.

Пятая глава посвящена актуальной тематике функциональной безопасности информационно – управляющих систем критически важными и ответственными объектами. Рассмотрены ключевые понятия состояния безопасности, функции и полноты безопасности. Изложены основные принципы функциональной безопасности, в том числе принципы отказобезопасности, избыточности, разнообразия и локализации развития неблагоприятных событий. Произведена оценка допустимого времени обнаружения одиночного и двойного опасных отказов. Описаны и проанализированы модели функциональной безопасности двухканальной системы со встроенными средствами диагностики и с внешним контролем. Рассмотрена проблема перезапуска каналов. Предложена и изучена модель для оценки вероятности возникновения опасных отказов при перезапуске двухканальных систем. Совместное применение разных информационных технологий построения информационных систем управления ответственными и критически важными объектами создает естественные условия для построения двухуровневой системы управления безопасностью. В двухуровневой системе возможно применение небезопасных систем. В главе приведены результаты математического моделирования различных стратегий построения двухуровневых информационных систем. Показано, что значительно эффективнее по сравнению с другими стратегиями является та, которая при наличии недостаточно безопасных составных систем позволяет рационально использовать естественную дополнительную информацию, имеющуюся по результатам предыдущих циклов управления.

В шестую главу включены принципы и методы подтверждения соответствия информационных систем требованиям Технических регламентов и нормативных документов. Приведены методы испытаний программных средств на соответствие требованиям качества и функциональной безопасности, а также безопасности информации. Рассмотрены вопросы практического применения методов испытаний программ. Особое внимание уделено проблеме ускорения испытаний. Описаны основные пути ускорения испытаний на основе понижения дисперсий получаемых показателей качества, надежности и безопасности испытуемых объектов: метод Монте-Карло и метод значимой выборки. Изложена инженерная методика ускоренных натурных испытаний на функциональную надежность и функциональную безопасность информационных систем управления ответственными или критически важными объектами, в том числе базовые теоретические положения этой методики, порядок проведения испытаний и оценка их продолжительности, порядок обработки результатов и формы представления данных. Приведен пример практического применения ускоренных натурных испытаний информационной системы диспетчерского управления на железнодорожном транспорте. Приведены основные положения методик испытаний программных средств по требованиям качества и функциональной безопасности и отсутствия недекларированных возможностей в программах, а также порядок подтверждения комплексной безопасности программных средств.

В конце каждой главы книги содержатся контрольные вопросы по наиболее сложному и значимому материалу главы. Книга рассчитана, в первую очередь, на специалистов, занимающихся практической работой по разработке, производству, эксплуатации и модификации информационных систем. Она предназначена научным работникам в области надежности программно – аппаратных систем, профессорско – преподавательскому составу, аспирантам и студентам, специализирующимся в области информационных технологий, в области информационных систем, а также в области автоматизированных систем управления.

Данная книга завершает проект из трех книг, предназначенный для представления широкой аудитории специалистов методов анализа структурной и функциональной надежности информационных систем и, особенно, методов синтеза надежности, отказоустойчивости и функциональной безопасности таких систем.