Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 8 (135)/2004

Функциональная безопасность программных средств

КОРПОРАТИВНЫЕ СИСТЕМЫ

Функциональная безопасность программных средств

В.В. Липаев[1],
профессор, доктор технических наук

СОДЕРЖАНИЕ

1) Об авторе: окончил физический факультет МГУ, доктор технических наук, профессор, главный научный сотрудник Института системного программирования РАН. Длительное время работал в Московском НИИ приборной автоматики, в последние годы - Главным конструктором и председателем Координационного совета Министерства радиопромышленности СССР по автоматизации проектирования программного обеспечения, руководителем комплексного проекта ПРОМЕТЕЙ по разработке автоматизированных технологий создания крупномасштабных программных средств для систем реального времени. Автор более тридцати монографий и методических руководств, а также 250 оригинальных статей и изобретений.

1. Проблемы обеспечения функциональной безопасности программных средств

Обязательные требования к продукции, производству и эксплуатации определены Федеральным Законом РФ «О техническом регулировании». В нем, в частности, **введено понятие безопасности** продукции – «состояние, при котором отсутствует недопустимый риск (вероятность), связанный с причинением вреда жизни и здоровью граждан, имуществу физических и юридических лиц, государственному или муниципальному имуществу, окружающей среде...». Там же определены основные понятия: технический регламент, техническое регулирование, стандартизация, сертификация, система сертификации, аккредитация, подтверждение соответствия и др., а также цели, принципы и порядок их практического применения.

В статье из всего многообразия сфер, в которых рассматривается и учитывается безопасность, выделена область применения систем обработки информации и управления реального времени, основой которых являются электронные вычислительные машины (ЭВМ), а также программные средства (ПС) и информационные ресурсы баз данных (БД). При этом под безопасностью продукции, процессов производства и эксплуатации систем понимается их работоспособное состояние и функционирование в соответствии с требованиями заказчика и технической документации, при которых **отсутствуют опасные отказы и недопустимый ущерб**.

В критических системах, в которых результаты обработки информации и управляющие воздействия непосредственно определяют работоспособность и качество функционирования сложных систем управления в чрезвычайных ситуациях, системами вооружения, космическими объектами, не исключены и изредка происходят **аварии и катастрофы вследствие недостаточной безопасности программных средств**. Имеется множество примеров гибели дорогих спутников или катастрофических ситуаций при применении сложных динамических объектов (Марс-1 – 1976г, Ариан-5 – 1997г, Апполон-13 – 1978 г и т.д.), а также больших финансовых и материальных потерь в авиации, в военных системах и на транспорте вследствие относительно простых ошибок в программах. В наиболее тяжелых случаях ущерб измерялся ценой жизни и здоровья людей или большими материальными потерями. В то же время они имели вполне объяснимую природу и источники, влияние которых могло быть снижено путем глубокого анализа, выявления дефектов и корректировок программ или информации баз данных.

Имеющиеся достижения в области теории и практики управления безопасностью сложной промышленной продукции, как правило, не известны и не используются специалистами, создающими и применяющими военные системы на базе программных средств. Это во многих случаях определяет дефекты и отказовые ситуации при применении ПС, конфликты между заказчиками и разработчиками из-за неопределенностей значений их безопасности и не конкурентоспособность создаваемых ПС на мировом рынке. Формализация и оценивание реальной безопасности программных средств и систем часто зависит от интуиции и квалификации их разработчиков, заказчиков и пользователей. В результате проекты ПС не соответствуют исходному, декларированному назначению и первоначальным спецификациям требований к характеристикам безопасности и качества, не укладываются в согласованные графики и бюджет разработки.

В требованиях технических заданий и реализованных проектах сложных систем и ПС, связанных с безопасностью, **систематически умалчиваются и/или недостаточно формализуются** понятия и метрики безопасности программного продукта и выдаваемой информации, какими характеристиками они должны описываться, как их следует измерять и сравнивать с требованиями, отраженными в контракте, техническом задании или спецификациях. Кроме того, некоторые из характеристик функциональной безопасности часто вообще отсутствуют в требованиях заказчика и согласованных документах на систему и ПС, что приводит к произвольному их учету или к пропуску при испытаниях. Этому способствует ограниченность ресурсов, необходимых для достижения и оценивания в процессах жизненного цикла комплексов программ, требуемых и реализованных значений безопасности, а также недостаточная формализация и документирование всего процесса их выбора и анализа.

Непрерывно возрастающая сложность и вследствие этого уязвимость систем и ПС от случайных и предумышленных негативных воздействий выдвинули ряд рассматриваемых ниже проблем, связанных с безопасностью систем, исполь-

зующих программные средства, в разряд важнейших – **стратегических**, определяющих принципиальную возможность и эффективность их применения. При этом выделились области анализа и обеспечения **информационной безопасности**, связанные, в основном, с защитой от предумышленных, негативных воздействий на информационные ресурсы систем, и **функциональной безопасности**, обусловленной отказовыми ситуациями и потерей работоспособности систем и ПС вследствие проявления непредумышленных, случайных дефектов программ, данных, аппаратуры и внешней среды.

Проблема обеспечения информационной безопасности функционирования ИС в процессе разработки и эксплуатации возникла и развивается вследствие возрастания сложности и ответственности задач использования информационных ресурсов и увеличения их уязвимости от предумышленных, внешних воздействий, с целью незаконного использования или искажения информации и программ, которые по своему содержанию предназначены для применения ограниченным кругом лиц [1, 3, 9, 11]. Основное внимание в современной теории и практике обеспечения безопасности информационных систем сосредоточено на защите от злоумышленных разрушений, искажений, хищений и использования программных средств и информации баз данных. Для этого разработаны и активно развиваются проблемно-ориентированные методы и средства защиты от несанкционированного доступа, от различных типов вирусов и закладок, от утечки информации по каналам электро-магнитного излучения и т.д. При этом подразумевается наличие лиц, заинтересованных в несанкционированном доступе к конфиденциальной или полезной информации в системах, с целью её незаконного использования. Для решения этой проблемы созданы и активно развиваются методы, средства и стандарты обеспечения информационной безопасности – защиты программ и данных от **предумышленных негативных внешних воздействий**.

Проблема обеспечения функциональной безопасности при случайных, дестабилизирующих воздействиях и отсутствии злоумышленного влияния на системы, ПС или информацию баз данных существенно отличается от задач информационной безопасности. При анализе функциональной безопасности рассматриваются опасные отказовые ситуации, приводящие к потере работоспособности систем, к авариям и катастрофам. При таких воздействиях внешняя функциональная работоспособность систем может разрушаться не полностью, однако невозможно полноценное выполнение заданных функций и требований к качеству информации для потребителей. В рассматриваемых ниже системах безопасность их функционирования определяется проявлениями дестабилизирующих факторов, приносящих большой ущерб:

- техническими отказами внешней аппаратуры и искажениями исходной информации от объектов внешней среды и от потребителей систем и обработанной информации;
- случайными отказами, сбоями и физическими разрушениями элементов и компонентов аппаратных средств вычислительных комплексов и средств телекоммуникации;
- дефектами и ошибками в комплексах программ обработки информации и в данных;
- пробелами и недостатками в средствах обнаружения опасных отказов и оперативного восстановления работоспособного состояния систем, программ и данных.

В реальных сложных системах, связанных с безопасностью, возможны катастрофические последствия и отказы функционирования с большим ущербом при **отсутствии враждебных лиц, заинтересованных в подобных нарушениях работоспособности систем и ПС**. Вредные и катастрофические последствия таких отказов в ряде областей применения систем могут превышать по результатам последствия злоумышленных воздействий, имеют свою природу, особенности и характеристики. Поэтому они требуют самостоятельного изучения и адекватных методов и средств обеспечения безопасности. В некоторых системах отказы, отражающиеся на функциональной безопасности, могут быть обусловлены нарушением информационной безопасности, предумышленным разрушением или искажением информации в базах данных. Тщательное **специфицирование и оценивание функциональной безопасности систем**, программного продукта и обработанной для потребителей информации – **ключевой фактор обеспечения их эффективного и адекватного применения**. Это может быть достигнуто на основе выделения, определения и обеспечения подходящих характеристик с учетом целей использования и функциональных задач ПС и систем.

При анализе характеристик функциональной безопасности целесообразно выделять **два класса систем и их ПС**. Первый класс составляют системы, имеющие встроенные комплексы программ жесткого регламента реального времени, автоматизировано управляющие внешними объектами или процессами. Время необходимой реакции на отказовые ситуации таких систем обычно исчисляется секундами или долями секунды, и процессы восстановления работоспособности должны проводиться за это время в достаточной степени ав-

томатизировано (бортовые системы в авиации, в некоторых средствах вооружения и транспорта). Системы второго класса применяются для управления процессами и обработки деловой информации из внешней среды, в которых активно участвуют специалисты-операторы (административные, банковские, штабные военные системы). Допустимое время реакции на опасные отказы в этих системах может составлять минуты, и операции по восстановлению работоспособности могут быть доверены специалистам-администраторам по обеспечению безопасности.

Понятия и характеристики функциональной безопасности систем близки к понятиям надежности. Основное различие состоит в том, что в показателях надежности учитываются все реализации опасных отказов, а в характеристиках функциональной безопасности следует регистрировать и учитывать только те отказы, которые привели к столь большому, катастрофическому ущербу, что отразилось на безопасности функционирования системы, на информации для потребителей или объектов управления. Статистически таких отказов может быть в несколько раз меньше, чем учитываемых в значениях надежности. Однако методы, влияющие факторы и реальные значения показателей надежности ПС могут служить ориентирами при оценке функциональной безопасности критических систем. Поэтому способы оценки и испытаний функциональной безопасности могут базироваться на концепции измерения надежности функционирования комплексов программ и баз данных.

Ущерб от дефектов и ошибок программ и данных может иметь куммулятивный характер и проявляться в систематических отказах, каждый из которых отражается на надежности, но не является катастрофой с большим ущербом, влияющим на безопасность системы. Накопление таких отказов со временем может приводить к последствиям, нарушающим функциональную безопасность систем и их применение. Таким образом, сближаются понятия надежности и функциональной безопасности сложных систем и ПС. При более или менее одинаковых источниках угроз и их проявлениях эти понятия можно разделить по величине последствий и ущерба при возникновении отказовых ситуаций.

Проблемы неопределенностей концепции функциональной безопасности конкретных систем, включающих программные средства, должны учитываться заказчиками, пользователями и разработчиками в течение всего их жизненного цикла. Чем сложнее системы и чем выше к ним требования безопасности, тем неопределеннее функции и характеристики их безопасности и качества. Неопределенности начинаются с требований заказчиков, которые при формулировке технического задания и спецификаций не полностью формализуют и принципиально не могут обеспечить содержание абсолютно всего набора функций, характеристик и их значений безопасности, которые должны быть при завершении проекта и предъявлении конечного продукта заказчику. Эти требования итерационно формируются, детализируются и уточняются по согласованию между всеми участниками проекта вследствие естественной ограниченности первичных исходных данных и изменения их под влиянием объективных и субъективных воздействий со стороны различных процессов на последовательных этапах ЖЦ.

Всегда не полностью, с необходимой детализацией определены и описаны все характеристики, особенности функционирования и безопасности объектов внешней среды. Эти характеристики в той или иной степени обычно находятся под воздействием управляемой системы и ПС. Сложность, а поэтому и неопределенность их представления, как правило, адекватны сложности всей системы, функциональная безопасность которой должна обеспечиваться в течение ее ЖЦ. Квалификация и субъективные свойства потребителей и пользователей изменяются по мере освоения функциональных возможностей системы и ее работоспособности, что увеличивает неопределенность ее реальной безопасности. Смена и различия персонала, применяющего систему и ПС, дополнительно увеличивает неопределенность значений безопасности и трудности ее прогнозирования с учетом множества субъективных факторов различных специалистов, участвующих в эксплуатации.

В процессе проектирования, разработки и всего жизненного цикла основных функциональных задач, операционной среды, аппаратуры ЭВМ эти компоненты с течением времени развиваются и адаптируются, что отражается на необходимости адекватного изменения методов, задач и средств обеспечения их функциональной безопасности. Таким образом, проблемы обеспечения функциональной безопасности сложных систем должны решаться с учетом одновременного динамического развития всех компонентов среды и факторов, непрерывно изменяющихся и воздействующих на результаты их решения. Однако такой сложный, непрерывный, многосвязный процесс трудно реализовать практически и его целесообразно решать поэтапно, возможно с необходимыми итерациями и упрощениями. При этом следует иметь в виду, что всегда могут проявиться отдаленные связи процессов, которые могут существенно повлиять на теку-

щие работы по обеспечению безопасности системы и ПС.

Роль негативных воздействий и их разрушительные последствия быстро возрастают в связи с ростом сложности разработки и применения современных систем на базе ЭВМ и ответственности решаемых ими задач. Одновременно возрастает сложность внешней и операционной среды, в которой функционируют ПС и ответственность систем, связанных с безопасностью. Объективное повышение сложности функций, реализуемых программами в современных системах, непосредственно приводит к увеличению их объема и трудоемкости создания. Соответственно росту сложности программ **возрастает относительное и абсолютное количество выявляемых и остающихся в них дефектов и ошибок**, что отражается на снижении потенциальной безопасности их функционирования. По мере увеличения сложности задач, решаемых программами, возрастает влияние ошибок, которые могут угрожать авариями и катастрофами в системах, выполняющих критические функции управления крупными, дорогими и особенно важными объектами или процессами.

Упорядоченное, регламентированное проектирование архитектуры, разработка и сопровождение сложных ПС на базе современных технологий позволяет предупреждать и устранять наиболее опасные системные, алгоритмические и программные дефекты и ошибки на ранних стадиях жизненного цикла, а также использовать неоднократно проверенные в других проектах безопасные программные и информационные компоненты. Для обеспечения безопасности критических систем необходимы эффективные методы и средства, предупреждающие и выявляющие дефекты, а также удостоверяющие безопасность использования программ и баз данных, оперативно защищающие их корректное функционирование при проявлении любых дефектов и отказовых ситуаций.

Работоспособность ПС может быть обеспечена при исходных данных, которые использовались при их разработке, отладке и испытаниях. Реальные исходные данные могут иметь значения, отличающиеся от предусмотренных техническим заданием и от используемых при эксплуатации программ и баз данных. При таких исходных данных функционирование ПС трудно предсказать заранее, и весьма вероятны различные аномалии, завершающиеся отказами, которые отражаются на безопасности. Следует учитывать принципиальные трудности аналитического оценивания и прогнозирования значений функциональной безопасности программных средств, вследствие непредсказуемости положения, проявления и последствий дефектов и ошибок в программах и данных. Это приводит к практической невозможности достоверных априорных аналитических расчетов функциональной безопасности комплексов программ при ее высоких значениях.

Проблема достижения требуемой функциональной безопасности систем, содержащих программные средства реального времени, решается путем использования **современных регламентированных технологических процессов** и инструментальных средств обеспечения их жизненного цикла [7, 10, 14]. Они должны быть поддержаны группой международных стандартов, определяющих состав и процессы выполнения требований к заданной функциональной безопасности систем и ПС. Структура, последовательность и содержание технологических процессов ЖЦ в этих стандартах несколько различаются, однако номенклатура базовых компонентов практически совпадает, что позволяет их выбирать и применять с учетом особенностей обеспечения безопасности конкретных проектов ПС.

Для систематической, координированной борьбы с угрозами безопасности ПС **необходимы исследования факторов, влияющих на функциональную безопасность со стороны случайных дефектов и ошибок**, существующих и потенциально возможных в конкретных системах и комплексах программ. Это позволит целенаправленно разрабатывать методы и средства обеспечения функциональной безопасности критических ПС различного назначения при реально достижимом снижении уровня дефектов проектирования и разработки. Проблема в значительной степени решается посредством применения современных методов, инструментальных средств и стандартов, поддерживающих системный анализ, технологию проектирования, разработки и сопровождения систем, их программных средств и баз данных.

Для создания безопасных систем и ПС, прежде всего, следует формализовать их назначение, функции и основные характеристики. На этой основе должны разрабатываться общие требования к функциональной безопасности и другим характеристикам качества ПС, к обработанной информации для потребителей, адекватной назначениям и функциям систем. Требования к функциям систем и ПС, а также к безопасности их функционирования должны соответствовать доступным ресурсам для их реализации с учетом допустимого ущерба — рисков вследствие отказов при неполном выполнении требований. **Ограниченности ресурсов** различных видов для обеспечения функциональной безопасности значительно влияют на технико-экономические показатели, качество и функ-

циональную безопасность всей системы и ПС. В результате сложность программ и баз данных, а также доступные ресурсы для их реализации становятся косвенными критериями или факторами, влияющими на выбор методов разработки, на достигаемое качество и безопасность ПС.

Для обеспечения безопасности ПС и результирующей информации для потребителей, необходимо освоение и применение современных методов, автоматизированных технологий и инструментальных средств, обеспечивающих **предотвращение или исключение большинства видов дефектов и ошибок** при создании и модификации ПС и их компонентов, обеспечивающих безопасность. Все этапы разработки и сопровождения ПС следует поддерживать методами и средствами верификации и систематического, автоматизированного тестирования модулей и компонентов программ. **Тестирование является основным методом** устранения дефектов, измерения и определения реальных характеристик программ на любых этапах их жизненного цикла. Наличие достаточно полных эталонов на основе совокупности требований спецификаций и поэтапная их декомпозиция — необходимая база тестирования и измерения реальной безопасности и качества комплексов программ. Ограниченность ресурсов при создании ПС приводит к целесообразности тщательного планирования, упорядочения и применения экономичных и эффективных методов автоматизации поэтапных испытаний в ЖЦ ПС с целью достижения требуемой функциональной безопасности и достоверного ее определения.

Разработку систем и ПС должны завершать **комплексные испытания и удостоверение достигнутой функциональной безопасности** и надежности систем с программными средствами, предусматривающие возможность совершенствования их характеристик путем соответствующих корректировок программ. Повышение функциональной безопасности целесообразно путем реализации процедур анализа выявленных дефектов и **оперативного восстановления вычислительного процесса, программ и данных** (рестарта) после обнаружения аномалий и отказов функционирования ПС. Этому может способствовать накопление, мониторинг и хранение данных о выявленных дефектах, сбоях и отказах в процессе исполнения программ и обработки данных.

2. Основные понятия и факторы, определяющие безопасность программных средств

Любые программные средства, прежде всего, должны иметь экономическую, техническую, научную или социальную эффективность применения, которая в проектах должна отражать основную **цель их жизненного цикла** в системе. Эта **системная эффективность** может быть описана количественно или качественно, в виде набора полезных свойств и характеристик ПС, их отличий от имеющихся у других комплексов программ, а также факторов и источников возможной эффективности. В результате должна быть формализована цель использования и набор требований заказчика и пользователей при создании или приобретении ПС, а также его предполагаемое назначение и сфера применения.

Системная эффективность применения программных средств определяется степенью удовлетворения потребностей определенных лиц — заказчиков и/или пользователей, которую во многих случаях желательно измерять экономическими категориями: прибылью, стоимостью, трудоемкостью, предотвращенным ущербом, длительностью применения и т.п. В стандартах эта эффективность отражается основной, обобщенной характеристикой качества — **функциональная пригодность ПС**. Данная характеристика связана с тем, **какие** функции и задачи решает ПС для удовлетворения потребностей пользователей, в то время как другие конструктивные характеристики (в том числе безопасность) главным образом связаны с тем, **как и при каких условиях** заданные функции могут выполняться с требуемым качеством. Номенклатура и значения всех конструктивных показателей качества непосредственно определяются требуемыми функциями программного средства и, в той или иной степени, влияют на выполнение этих функций. Поэтому выбор и формализация функциональной пригодности ПС, подробное и корректное описание ее свойств являются основными исходными данными для установления при проектировании требуемых значений всех остальных стандартизированных показателей качества.

Стандартизированные в **ISO 9126** характеристики качества ПС различаются по степени влияния на системную эффективность применения комплексов программ по прямому назначению. Высшие приоритеты, естественно, должны присваи-

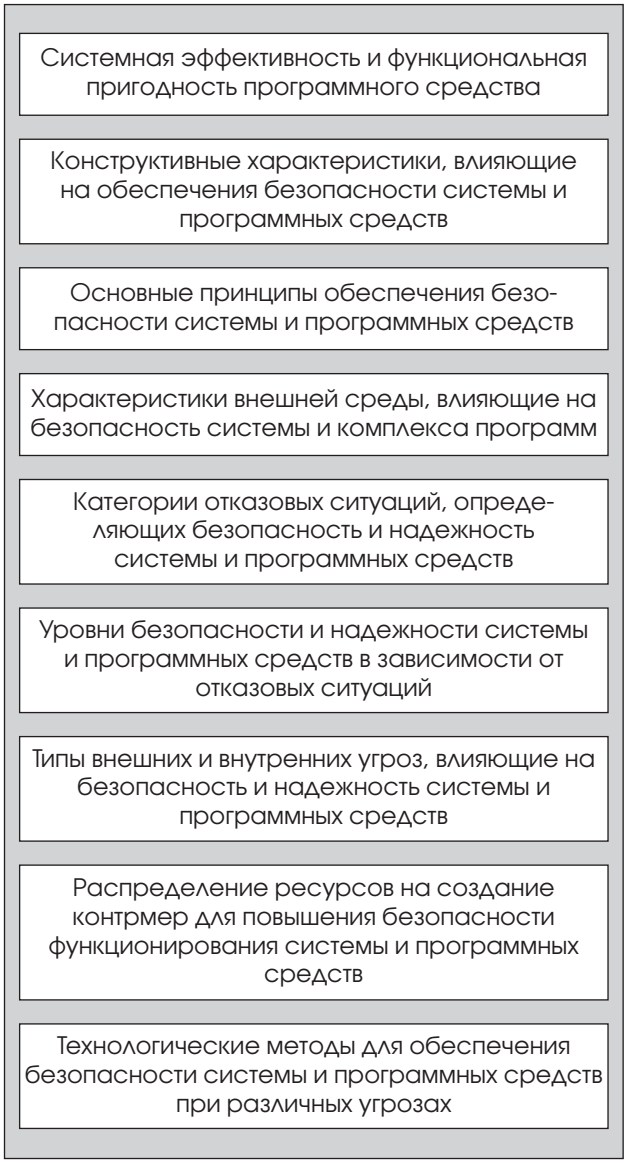

Рис. 1

ваться свойствам и атрибутам функциональной пригодности, необходимым для достижения основных **стратегических целей** использования ПС. Все остальные стандартизированные характеристики ПС должны способствовать обеспечению **тактических целей** выбранных конструктивных требований. Решение этих задач должно быть направлено на обеспечение высокой функциональной пригодности ПС **путем сбалансированного улучшения остальных конструктивных характеристик качества (и безопасности) в условиях ограниченных ресурсов на ЖЦ**. Для этого в процессе системного анализа при подготовке технического задания и требований спецификаций, значения различных факторов, характеристик качества и безопасности должны выбираться с учетом их влияния на функциональную пригодность. На рис. 1 представлена основная совокупность факторов и действий по обеспечению функциональной безопасности систем и ПС.

Улучшение каждой вспомогательной — **конструктивной характеристики качества**, в том числе безопасности, требует некоторых затрат ресурсов (трудоемкости, финансов, времени), которые в той или иной степени должны отражаться на основной характеристике качества — на функциональной пригодности. В зависимости от назначения и функций ПС почти каждая из конструктивных характеристик может стать доминирующей или даже почти полностью определяющей функциональную пригодность ПС. В наибольшей степени функциональная пригодность во многих случаях зависит от **безопасности и надежности ПС**.

Цели, назначение и функции защиты комплекса программ от отказов тесно связаны с особенностями функциональной пригодности каждого типа ПС. Разработка и формирование требований к свойствам и характеристикам безопасности должны осуществляться на основе потребностей эффективной реализации назначения и основных функций ПС при различных, реальных угрозах. В процессе системного анализа и проектирования должны быть выявлены потенциальные предумышленные и случайные угрозы функционированию ПС и установлен **необходимый уровень безопасности** данного комплекса программ. В соответствие с этим уровнем, заказчиком и разработчиками должны выбираться и устанавливаться требуемые и необходимые наборы методов, свойств и средств обеспечения безопасности ПС с учетом ограниченных ресурсов на их реализацию. В результате сформированные требования должны обеспечивать равнопрочную защиту от различных реальных угроз и реализацию необходимых мер контроля и подтверждения требуемых характеристик функциональной пригодности комплекса программ в условиях угроз безопасности функционирования ПС [3, 4, 12].

Для обеспечения эффективности системы, **комплекс программ, связанный с безопасностью, целесообразно базировать на следующих общих принципах**:

- защита аппаратуры системы, функциональных программ и данных должна быть комплексной и многоуровневой, ориентированной на все виды угроз с учетом их опасности для потребителя;
- стоимость (трудоемкость) создания и эксплуатации системы программной защиты должна быть меньше, чем размеры наиболее вероятного или возможного (в среднем) неприемлемого потребителями системы ущерба — риска от любых потенциальных угроз;
- комплекс программ защиты должен иметь целевые, индивидуальные компоненты контрмер, предназначенные для обеспечения безо-

пасности функционирования каждого отдельно взятого компонента и функциональной задачи системы с учетом их уязвимости и степени влияния на безопасность системы в целом;
- система программ защиты не должна приводить к ощутимым трудностям, помехам и снижению эффективности применения и решения основных, функциональных задач пользователями системы в целом.

Характеристики внешней среды, прикладные сферы применения комплексов программ, цели и задачи пользователей, уровень автоматизации их функций и многие другие факторы определяют методы и свойства средств обеспечения безопасности вычислительных систем. Различие между видами безопасности не всегда достаточно четкое и его следует рассматривать и учитывать в зависимости от конкретных функций систем и ПС, задач и результатов обеспечения безопасности, а также от категорий и характеристик возможных отказовых ситуаций. При последующем анализе внимание акцентируется на определении требований и применении сложных аппаратно-программных систем и на их **функциональной безопасности**. Соответственно ущерб при отказовых ситуациях определяется уязвимостью и нарушением корректного выполнения системой основного назначения и требуемых функций при ограниченных ресурсах на их реализацию. Контрмеры при этом ограничиваются дополнительными средствами защиты от отказов, изменением соотношений требований к различным характеристикам ПС и перераспределением доступных ресурсов для их реализации.

Функции систем и их программных средств реализуются в определенной аппаратной, операционной и пользовательской внешней среде, характеристики которых существенно влияют на функциональную пригодность программ. Для выполнения требуемых функций комплекса программ необходима **адекватная исходная информация от объектов внешней среды**, содержание которой должно полностью обеспечивать реализацию функций, декларированных в требованиях к системе. Полнота формализации номенклатуры, структуры и качества входной информации для выполнения требуемых функций, является одной из важных составляющих при определении функциональной пригодности ПС в соответствующей внешней среде.

Требования к **функциональной безопасности системы** проистекают из целей **обеспечения безопасности объектов и их компонентов**, реализующих назначение и основные функции системы, а также из целей обеспечения **безопасности её среды**. Такое разделение основано на совокупном учете инженерного опыта, политики безопасности, экономических факторов и анализа рисков. Требования безопасности являются результатом преобразования общих целей безопасности системы в совокупность требований безопасности для функциональных объектов и требований безопасности для внешней среды, которые, в случае их удовлетворения, должны обеспечить для системы и ПС способность достижения его базовых целей функциональной безопасности.

Так как без дефектов и ошибок принципиально невозможно создать и применять сложные комплексы программ, эти проблемы должны направленно изучаться и обобщаться в некоторую совокупность знаний — **«дефектологию ПС»**. В ней следует оценивать свойства, содержание и характеристики дефектов и ошибок в ПС, их проявления и негативные последствия для потребителя, угрозы и ущерб для безопасности функционирования системы в целом. Внимание должно быть сосредоточено на характеристиках дефектов функциональных программ, определяющих **основное назначение системы**.

Среда обеспечения функциональной безопасности ПС включает политики и программы организации безопасности предприятий и систем, опыт, специальные навыки и знания, определяющие контекст предполагаемого применения системы. Среда включает также возможные угрозы безопасности, присутствие которых в этой среде установлено или предполагается. При формализации среды функциональной безопасности следует принимать во внимание:
- предназначение системы и ПС, включая функции продукта и предполагаемую сферу его применения;
- активы — программы и данные функциональных задач системы, которые требуют обеспечения безопасности, к которым применяются требования и/или политики безопасности, а также компоненты, которые подчинены требованиям безопасности системы и ПС;
- физическую среду в той её части, которая определяет все аспекты эксплуатационной среды системы, касающиеся безопасности, включая мероприятия, относящиеся к средствам физической защиты и к персоналу.

На основании разработанных политик безопасности, оценок угроз и рисков следует сформировать исходные данные, **относящиеся к функциональной безопасности** среды системы и основного комплекса программ:
- предположения, которым должна удовлетворять среда для того, чтобы система или ПС считались безопасными;

- угрозы безопасности для активов, в которых были бы идентифицированы все угрозы среды, прогнозируемые на основе анализа безопасности как относящиеся к объекту функциональной безопасности;
- угрозы, которые раскрываются через понятия источника угроз, предполагаемого метода их реализации, предпосылки для отказов и идентификация компонентов, которые являются объектами отказов;
- политика безопасности, в которой были бы достаточно точно идентифицированы и описаны цели, методы и правила реализации функциональной безопасности системы.

Результаты анализа среды безопасности могут использоваться для формулирования целей функциональной безопасности системы, которые направлены на противостояние установленным угрозам, а также проистекают из политики безопасности предприятия или проекта и сделанных предположений. Необходимо, чтобы общие цели безопасности системы были согласованы с определенными ранее целями применения и характеристиками функциональной пригодности системы или ПС как продукта, а также со всеми известными сведениями о внешней среде системы.

Основные понятия в области функциональной безопасности систем и программных средств характеризуются факторами, связанными с возникновением опасных состояний, приводящих к **потере работоспособности**. Если эти события не обнаруживаются и не устраняются специально введенными в состав системы средствами обеспечения безопасности, то возникают опасные отказы и их последствия. Систему, в состав которой требуется вводить функции безопасности, принято называть **системой, связанной с безопасностью**. Эти функции необходимы для достижения или поддержания безопасного состояния объекта управления или обработки информации — самостоятельно или совместно с другими, **связанными с безопасностью системами**, а также с внешними средствами снижения риска для предотвращения или смягчения последствий опасного события.

Примерами могут служить ПС систем, связанные с безопасностью управления движением самолета, автомобиля, систем электрической и диспетчерской централизации на железной дороге, средств управления атомными реакторами и т.д. Иными словами, любое программное средство, отказ которого может повлиять на возникновение аварийной или катастрофической ситуации, последствиями которой может быть тот или иной ущерб, следует считать связанным с безопасностью. Человек может являться компонентом такой системы, например, получать информацию от программируемого электронного устройства и выполнять действия по обеспечению безопасности на основе этой информации или же он может выполнять действия по обеспечению безопасности, используя такое устройство.

Термины, используемые далее и связанные с функциональной безопасностью систем и ПС, аналогичны тем, которые содержатся в стандартах **ГОСТ 27.002 – 89**, **IEC 61508**, **ISO 15408** и др. Эти определения базируются на понятии отказа как события, заключающегося в нарушении работоспособного состояния объекта. Определение отказа является базовым для оценки функциональной безопасности и надежности технических систем:

- **работоспособное состояние** — при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют требованиям нормативно — технической и/или конструкторской и проектной документации;
- **неработоспособное состояние** — при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции, не соответствует требованиям нормативно — технической и/или конструкторской и проектной документации;
- **отказовая ситуация** — скрытый отказ, не обнаруживаемый визуально или штатными методами и средствами контроля и диагностирования, но выявляемый средствами автоматизированного рестарта, а также при проведении технического обслуживания или специальными методами диагностики, который потенциально может превратиться в отказ;
- **отказ** — событие, заключающееся в нарушении работоспособного состояния системы;
- **опасный отказ** — событие, заключающееся в нарушении работоспособного или защитного состояния с большим ущербом;
- **дефекты аппаратуры, программы или данных** — негативные события, заключающиеся в непреднамеренном отклонении от требований спецификации или документации в процессах их жизненного цикла;
- **ошибки аппаратуры, программ или данных** — случайные, непредсказуемые искажения компонентов или ПС, проявляющиеся в процессах их анализа или функционирования.

Для оценивания свойств функциональной безопасности и надежности систем и ПС необходимо регистрировать, измерять, обобщать и упорядочивать реальные характеристики отказовых ситуа-

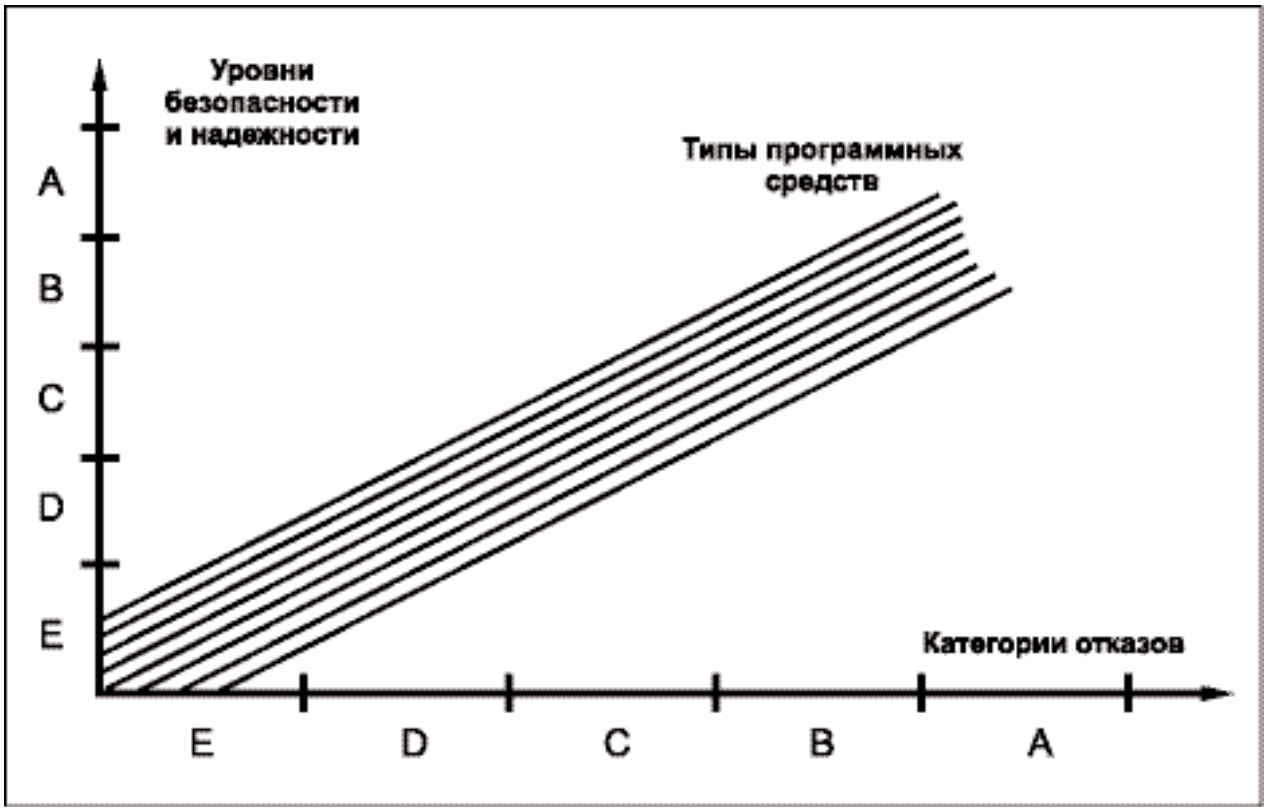

Рис. 2

ций и их последствия для безопасности. С этой целью в стандарте **ГОСТ Р 51904** рекомендуются **категории отказовых ситуаций систем и ПС**, в зависимости от серьезности их влияния на качество функционирования программ или данных объекта управления [8]. Необходимый для безопасного функционирования уровень качества ПС рекомендуется определять исходя из **опасности** отказовых ситуаций и возможного при этом **ущерба** для программ, системы и потребителя. Стандартом установлена следующая классификация отказовых ситуаций (рис. 2):

- **категория А – катастрофическая:** отказовая ситуация, которая препятствует полной работоспособности и функционированию системы или ПС в соответствии с требованиями и способна нанести недопустимый по последствиям и величине ущерб системе или пользователям;
- **категория В – опасная/критическая:** отказовая ситуация, которая приводит к значительному снижению работоспособности, возможностей применения и функционирования системы или к отсутствию способности персонала справиться с неблагоприятными эксплуатационными режимами, при которых возникают:
  - крайне тяжелые ситуации или перегрузки системы, которые могут вызвать неточное или неполное выполнение основных, функциональных задач с большим ущербом;
  - недопустимо большое снижение характеристик функциональной пригодности, реализуемых функций и конструктивных характеристик качества системы или ПС;
  - неблагоприятные или потенциально фатальные воздействия системы или ПС для окружающей внешней среды;
- **категория С – существенная:** отказовая ситуация, которая приводит к снижению возможностей применения и функциональной пригодности системы или к сокращению способности персонала справиться с неблагоприятными эксплуатационными режимами, при продолжении которых может возникать, например, большое искажение информационных ресурсов или сокращение функциональных возможностей, перегрузки или условия, вызывающие существенное ухудшение работоспособности системы или персонала;
- **категория D – несущественная:** отказовая ситуация, незначительно уменьшающая безопасность функционирования и применения объекта, но отражающаяся на его надежности или требующая действий персонала, которые осуществимы в пределах их возможностей для восстановления нормальной работоспособности, такая ситуация может включать в себя, на-

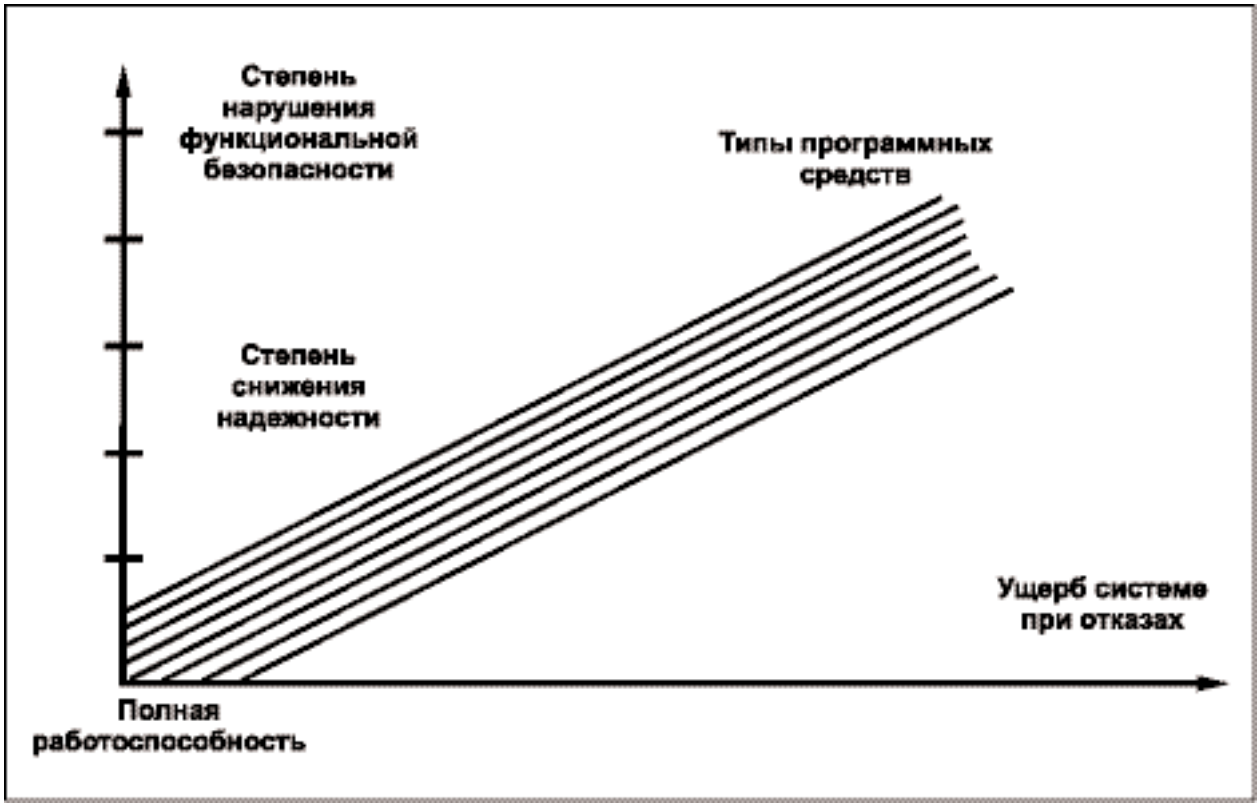

Рис. 3

пример, некоторое увеличение рабочей нагрузки, неудобство применения или задержки информации для персонала;

- **категория Е – невлияющая:** отказовая ситуация, которая практически не воздействует на работоспособность, эксплуатационные характеристики и возможности объекта или не увеличивает рабочую нагрузку персонала.

Эти пять категорий отказовых ситуаций отражают различную степень их влияния на качество функционирования систем или ПС, которое целесообразно распределить между понятиями **безопасность** и **надежность** в зависимости от возможного ущерба – риска при отказах [1, 8, 13]. Первые две категории ситуаций характеризуются большими значениями ущерба при отказах и их следует рассматривать с позиции классов безопасности функционирования систем. Две последние категории практически не влияют на безопасность применения объектов, но отражаются на надежности их функционирования с относительно невысоким ущербом. Такие отказовые ситуации не целесообразно рассматривать с позиции безопасности. К наиболее сложному случаю относится третья – существенная категория отказовых ситуаций. Она требует детального и конкретного анализа функциональных характеристик системы, ПС и отказов, которые могут отражаться не только на надежности, но и в той или иной степени влиять на безопасность функционирования системы.

Можно предположить для простоты, что уровни функциональной безопасности и надежности линейно зависят от категории отказов и несколько отличаются для различных типов программных средств (см. рис. 2). Эти зависимости можно интерпретировать, как снижение работоспособности системы или ПС в результате проявления некоторого ущерба – риска. Ущерб при отказах проявляется либо в снижении надежности при функционировании, либо, в худшем случае, как нарушение функциональной безопасности (рис. 3). Таким образом, категории отказовых ситуаций, величина ущерба – риска, трудоемкость и длительность восстановления нормального функционирования системы могут рассматриваться как база для оценивания и категоризации **пороговых уровней** в требованиях к безопасности и/или надежности функционирования и применения систем и их программных средств.

Уровни безопасности и надежности функционирования систем и ПС стандартом рекомендуется устанавливать в соответствии с категориями наиболее вероятных и опасных отказовых ситуаций в анализируемой или проектируемой системе. Уровень качества ПС также определяется возможностью возникновения потенциальных отказовых ситуаций, в результате сбоев в программах и данных, выявляемых средствами и процессами оценки безопасности. Это означает, что трудозатраты, ресурсы и время, необходимые для обеспечения со-

гласованности с требованиями заказчика к качеству функционирования, меняются в зависимости от категорий отказовых ситуаций (см. рис. 3):

- **уровень A:** программное средство, аномальное функционирование которого, как показано процессом оценки безопасности и качества системы, может вызвать возникновение отказа ее функционирования, приводящее к катастрофической отказовой ситуации и к полной функциональной непригодности системы с недопустимым ущербом – риском;
- **уровень B:** программное средство, аномальное поведение которого может вызвать возникновение критической отказовой ситуации, опасной для функциональной пригодности системы с большим ущербом – риском;
- **уровень C:** программное средство, аномальное поведение которого при оценке качества системы может способствовать возникновению существенной отказовой ситуации со средним ущербом – риском или значительному снижению функциональной пригодности и надежности;
- **уровень D:** программное средство, аномальное функционирование которого при оценке качества системы способствует возникновению несущественной отказовой ситуации для системы и малому ущербу – риску, влияющему только на некоторое снижение характеристик функциональной пригодности и надежности при применении;
- **уровень E:** программное средство, аномальное поведение которого практически не влияет на работоспособность и основные эксплуатационные возможности системы, работу персонала и риски функционирования, но возможно несколько снижает надежность и качество системы при применении.

Наиболее полно **степень функциональной безопасности систем характеризуется величиной предотвращенного или остаточного ущерба – риска**, возможного при проявлении дестабилизирующих факторов и реализации конкретных угроз безопасности применения системы и ПС пользователями. С этой позиции затраты ресурсов разработчиками и заказчиками на обеспечение безопасности системы должны быть соизмеримыми с возможным средним ущербом у пользователей от нарушения безопасности. Однако описать и измерить в достаточно общем виде возможный ущерб – риск при нарушении безопасности для критических ПС разных классов весьма сложно. Перечисленные выше отказовые ситуации и уровни функциональной безопасности могут быть следствием различных, **негативных явлений** в системе, которые в основном оцениваются:

- величиной экономического, материального или социального ущерба системе вследствие возникновения отказовой ситуации;
- трудоемкостью устранения последствий отказовой ситуации и восстановления нормальной работоспособности системы в соответствии с требованиями после отказа;
- длительностью неработоспособного состояния системы вследствие каждого отказа до полного восстановления работоспособности;
- затратами ресурсов и времени, необходимыми после отказа для восстановления нормальной работоспособности системы в соответствии с требованиями.

Реализации угроз, в ряде случаев, целесообразно характеризовать интервалами времени между их проявлениями, нарушающими безопасность применения ПС, или **наработкой на отказы**, отражающиеся на безопасности. Это сближает понятия и характеристики степени безопасности с показателями надежности системы. Различие состоит в том, что в показателях надежности учитываются все реализации отказов, а в характеристиках безопасности следует регистрировать только те катастрофические, критические или опасные отказы, которые отразились на нарушении безопасности с большим ущербом. Кроме того, в некоторых случаях последствия отказов может быть полезным отражать длительностью работоспособного состояния системы между событиями отказов относительно общей длительности применения системы с учетом затрат времени на обнаружение и ликвидацию отказов (коэффициент готовности системы).

Значения функциональной безопасности и надежности **коррелированны с характеристикой корректность ПС**, однако можно достигнуть высокой безопасности функционирования программ при относительно невысокой их корректности за счет автоматизации сокращения ущерба и времени восстановления при отказах. Степень покрытия тестами структуры функциональных компонентов и ПС в целом при разработке и испытаниях может служить ориентиром для прогнозирования их потенциальной безопасности. Распределение реальных длительностей и эффективности восстановления при ограниченных ресурсах для функционирования программ может рассматриваться как дополнительная составляющая при оценивании функциональной безопасности.

В требованиях к каждой конкретной системе должны быть установлены заказчиком совместно с пользователем **пороговые значения**, разделяющие

виды и величины ущерба, а также характеристики восстановления, которые следует относить либо к нарушению функциональной безопасности, либо только к снижению надежности. Однако методы их оценивания и измерения могут быть подобными. Эти пороговые значения зависят от назначения и базовых характеристик, отражающих функциональную пригодность конкретной системы или программного средства. При малом (ниже порога) ущербе вследствие отказовой ситуации и быстром восстановлении такие события следует относить к **снижению надежности**. Если последствия отказовых ситуаций какой-либо вид ущерба или характеристики восстановления превышают заданный критический порог, то такие события относятся к **нарушению функциональной безопасности** (см. рис.3). При этом в ряде ситуаций для нарушения безопасности может быть достаточным нарушение порогового значения одним из видов отказа. Если аномальное поведение компонента или системы может быть вызвано более чем одной отказовой ситуацией, уровень безопасности ПС следует определять по наиболее серьезной категории отказовой ситуации. Ниже при описании методов испытаний программных средств, для сокращения применяются преимущественно термины «функциональная безопасность» или «безопасность», при этом подразумевается, что так же может оцениваться их надежность.

В основу формирования требований к функциональной безопасности должно быть положено определение **перечня и характеристик потенциальных угроз безопасности** и установление возможных источников их возникновения [3, 10, 11]. **Внешними дестабилизирующими факторами**, создающими угрозы безопасности функционированию систем и ПС, являются:

- предумышленные, негативные воздействия лиц с целью искажения, уничтожения или хищения программ, данных и документов системы и ПС, как последствия нарушения информационной безопасности, отражающиеся также на функциональной безопасности;
- ошибки и несанкционированные воздействия оперативного, административного и обслуживающего персонала в процессе эксплуатации системы и ПС;
- искажения в каналах телекоммуникации информации, поступающей от внешних источников и передаваемой потребителям, а также недопустимые значения и изменения характеристик потоков информации от объектов внешней среды;
- сбои и отказы в аппаратуре вычислительных средств;
- вирусы, сбои и отказы, распространяемые по каналам телекоммуникации, влияющие на информационную и функциональную безопасность;
- изменения состава и конфигурации комплекса взаимодействующей аппаратуры системы или ПС за пределы, проверенные при испытаниях или сертификации.

Внутренними источниками угроз безопасности функционирования системы и ПС являются:

- системные ошибки при постановке целей и задач проектирования функциональной пригодности ПС и системы при формулировке требований к функциям и характеристикам средств обеспечения безопасности решения задач;
- дефекты и ошибки при определении функций, условий и параметров внешней среды, в которой предстоит применять защищаемые программные средства и систему;
- алгоритмические ошибки проектирования при непосредственной алгоритмизации функций обеспечения безопасности аппаратуры, программных средств и баз данных при определении структуры и взаимодействия компонентов функциональных комплексов программ, а также при использовании информации баз данных;
- ошибки и дефекты программирования в текстах программ и описаниях данных, а также в исходной и результирующей документации на компоненты ПС;
- недостаточная эффективность используемых методов и средств оперативной защиты программ и данных, обеспечения безопасности функционирования и восстановления работоспособности системы в условиях случайных и предумышленных негативных воздействий от внешней среды.

Полное устранение перечисленных выше угроз безопасности функционирования критических систем принципиально невозможно. При создании сложных комплексов программ проблема состоит в выявлении факторов, от которых они зависят, в создании методов и средств уменьшения их влияния на безопасность. Необходимо **оценивать уязвимость** функциональных компонентов системы для различных, негативных воздействий и степень их влияния на основные характеристики качества и безопасности, а также на суммарный риск. В зависимости от этого следует **распределять ресурсы** для создания системы и ее компонентов, равнопрочных по безопасности функционирования с минимальным обобщенным риском при любых негативных внешних воздействиях. В результате должны быть

сформулированы соответствующие методы и контрмеры, которые, в свою очередь, определяют необходимые функции и механизмы средств обеспечения работоспособности и безопасности.

Для обеспечения функциональной безопасности систем создаются **соответствующие контрмеры** – специализированные системы и средства, которые включают совокупность взаимосвязанных нормативных документов, организационно-технических мероприятий и соответствующих им методов и программных средств, предназначенных для предупреждения и/или ликвидации негативных последствий отказовых ситуаций, различных угроз безопасности, их выявления и локализации. Создание таких комплексов повышения безопасности предусматривает **планирование и реализацию целенаправленной политики** комплексного обеспечения функциональной безопасности системы, а также **эффективное распределение ресурсов на контрмеры и средства обеспечения безопасности**. Разработчики и заказчики должны анализировать возможные угрозы, чтобы решать, какие из них действительно присущи внешней среде, системе и ПС. Контрмеры предпринимают для уменьшения уязвимостей и выполнения политики безопасности. Но и после введения этих контрмер могут сохраняться остаточные риски, которые допустимы вследствие ограниченности ресурсов.

Требования к программным средствам, обеспечивающим безопасность, обычно представляются в составе общей спецификации требований к функциональной пригодности системы и ПС. В этом случае должны быть предприняты меры для **распределения системных требований к защите** между аппаратными и программными компонентами обеспечения функциональной безопасности. Если программная система обеспечения безопасности нуждается во взаимодействии с другими программными или аппаратными компонентами, то в спецификации требований должны быть оговорены непосредственно или при помощи ссылок интерфейсы между применяемыми составляющими.

Для прямых количественных измерений функциональной безопасности необходимы инструментальные средства, встроенные в операционную систему или в соответствующие компоненты и функции ПС. Эти средства должны в динамике реального функционирования ПС автоматически селектировать и регистрировать отказовые ситуации, дефекты и искажения вычислительного процесса программ и данных, выявляемые аппаратным, программно-алгоритмическим контролем или пользователями. Накопление и систематизация проявлений отказов при исполнении программ позволяет оценивать основные показатели безопасности, помогает определять причины сбоев и отказов и подготавливать данные для улучшения функциональной безопасности ПС. Регулярная регистрация и обобщение таких данных способствует устранению ситуаций, негативно влияющих на функциональную пригодность и другие базовые характеристики ПС.

Доступная величина и распределение ресурсов ЭВМ на отдельные виды контрмер оказывают значительное влияние на достигаемую комплексную безопасность системы. Наиболее общим видом ресурсов, который приходится учитывать при проектировании, являются **допустимые финансово-экономические затраты или трудоемкость разработки и функционирования комплекса средств обеспечения безопасности системы**. Для размещения этих средств в объектной ЭВМ, при проектировании должна быть предусмотрена программная и информационная избыточности в виде ресурсов внешней и внутренней памяти ЭВМ. Кроме того, для их функционирования необходима временная избыточность – дополнительная производительность ЭВМ. Эти **виды вычислительных ресурсов при обеспечении функциональной безопасности** используются также для:

- контроля и корректировки искажений информации, поступающей от внешней среды и источников данных;
- оперативного контроля и обнаружения дефектов исполнения программ и обработки данных при использовании ПС по основному назначению;
- размещения и обеспечения функционирования применяемых средств защиты от всех видов угроз безопасности системы;
- генерации тестовых наборов или хранения тестов для контроля работоспособности, сохранности и целостности ПС при функционировании системы;
- накопления, хранения и мониторинга данных о выявленных инцидентах, попытках несанкционированного доступа к информации, о дефектах, сбоях и отказах в процессе исполнения программ и обработки данных, влияющих на безопасность;
- реализации процедур анализа и мониторинга выявленных дефектов и оперативного восстановления вычислительного процесса, программ и данных (рестарта) после обнаружения дефектов и отказов функционирования системы.

Потребителя-заказчика, прежде всего, интересуют **функции, безопасность и качество готового конечного продукта** – системы и программного средства, и обычно не очень беспокоит, как они достигнуты. Требуемую функциональную безо-

пасность при разработке системы и ПС, как и любой продукции, можно обеспечить **двумя методами** [7, 10, 14]:

- путем использования только заключительного, выходного контроля и **испытаний** готовых объектов и исключения из поставки или направлением на доработку продуктов, не соответствующих требуемым безопасности и качеству;
- посредством применения регламентированных технологий и систем обеспечения функциональной безопасности и качества в процессах проектирования, разработки и изготовления, предотвращающих дефекты и гарантирующих высокую безопасность и качество продукции во время ее создания и/или модификации.

Первый метод может приводить к значительным экономическим потерям за счет затрат на создание части не пригодного к использованию брака, что может быть очень дорого для сложных систем. Достижение необходимой безопасности за счет только выходного контроля и испытаний, при отсутствии адекватной технологии и системы обеспечения качества в процессе разработки, может приводить к длительному итерационному процессу массовых доработок и повторных испытаний продукции.

Второй метод обеспечивает высокое качество выполнения всего процесса проектирования, разработки и изготовления и, тем самым, минимум экономических потерь от брака, что более рентабельно при создании сложных систем. При этом сокращается, но не исключается выходной контроль функциональной безопасности и качества продукции. Для создания современных прикладных высококачественных, безопасных систем необходимы оба метода с акцентом на применение регламентированных технологий. Таким образом, **политика обеспечения и удостоверения безопасности и качества сложных ПС должно базироваться на проверках и испытаниях**:

- технологий обеспечения жизненного цикла программных средств, поддержанных регламентированными системами качества;
- функционирования готового программного продукта с полным комплектом адекватной эксплуатационной документации.

Глубокая взаимосвязь качества разработанных систем и программ с качеством технологии их создания и с затратами на весь жизненный цикл становится особенно существенной при необходимости получения конечного продукта с предельно высокими значениями показателей безопасности и качества. Установлено, что затраты на разработку резко возрастают, когда показатель качества приближается к пределу, достижимому при данной технологии и уровне автоматизации процесса разработки. Это привело к существенному **изменению методологии и культуры в области создания и совершенствования систем и ПС**. Непрерывный рост требований к функциональной безопасности и качеству ПС стимулировали создание и активное применение международных стандартов и регламентированных технологий, автоматизирующих процессы всего жизненного цикла, начиная с инициирования проекта.

Экспериментальное определение и прямое измерение **величины реальной функциональной безопасности** сложных систем и комплексов программ в большинстве случаев затруднены необходимостью учитывать и оценивать очень редкие катастрофические отказовые ситуации. Для этого приходится проводить длительные эксперименты с созданием критических и опасных ситуаций эксплуатации систем, что может быть связано с большим риском и весьма дорого. Кроме того, редкие и одиночные отказовые ситуации не позволяют оценить статистически достоверные значения длительностей наработки на отказы и величины вероятного ущерба при этом. Аналитические расчеты и экспертные оценки величины функциональной безопасности комплексов программ усложняют случайное, непредсказуемое размещение дефектов и ошибок в программных модулях и компонентах, которые могут полностью определять функциональную безопасность.

Поэтому высокая функциональная безопасность программных продуктов достигается и определяется преимущественно за счет технологий обеспечения качества на всех этапах жизненного цикла систем и ПС. Для этого в стандартах, регламентирующих функциональную безопасность систем и комплексов программ, значительное **внимание уделяется технологическим процессам и инструментальным системам обеспечения безопасности** и качества ЖЦ ПС [7, 8, 9]. В стандарте **IEC 61508** третья и шестая части полностью посвящены требованиям и регламентированию процессов обеспечения функциональной безопасности встроенных комплексов программ аппаратно-программных систем. Жизненный цикл процессов обеспечения безопасности ПС структурирован схемой этапов и работ, компонентов и объектов, а также снабжен рекомендациями по выбору и реализации методов создания безопасных ПС. Третья часть стандарта **ISO 15408** почти целиком посвящена детальным требованиям по обеспечению гарантий качества

при создании и применении систем информационной безопасности комплексов. Совокупность этих требований отражает традиционные методы технологии поддержки жизненного цикла сложных ПС с акцентом на особенности реализации функций безопасности, которые применимы и для обеспечения функциональной безопасности. Технологии и типовые процессы создания безопасных систем и программных средств отражены также в стандартах **ISO 13335** и **IEC 60880**. Таким образом, значительная часть требований стандартов, посвященных функциональной безопасности, **акцентирована на технологических процессах** создания безопасных систем и программных средств, однако без выделения и описания процессов измерения достигаемых при этом критериев безопасности программных продуктов.

3. Характеристики среды, для которой должна обеспечиваться функциональная безопасность программных средств

Функциональная безопасность необходима не для всех классов современных систем и прикладных программных средств. Для конкретизации области дальнейшего анализа целесообразно выделить и установить **обобщенные характеристики и атрибуты рассматриваемых критических ПС** в соответствии со стандартом **ISO 12182** — (Классификация программных средств), для которых целесообразно обеспечивать функциональную безопасность. В стандарте выделены три группы видов характеристик: внутренние виды; виды среды и виды данных. Для каждого вида представлен перечень классов, из которых рекомендуется выбирать подходящие характеристики для отражения особенностей конкретной системы или для достаточно широкой сферы применения ПС. Из общего числа трех видов, 16-ти классов и около ста типов характеристик ПС **для обеспечения их функциональной безопасности далее будут учитываться следующие**:

- функции прикладных ПС — системы управления объектами или процессами;
- прикладная область системы — оборудование и аппаратура управления процессами и объектами;
- режим эксплуатации — обработка данных в режиме реального времени;
- масштаб, объем ПС — средний или большой;
- представление данных — предметный или объектный;
- критичность ПС — высокая, возможность повреждение дорогой собственности или угроза человеческой жизни;
- класс пользователей — технические средства и квалифицированные специалисты;
- стабильность ПС — маловероятное или дискретное внесение изменений;
- готовность программного продукта — заказное для конкретного применения в системе;
- требуемые рабочие характеристики: емкость памяти — средняя или низкая; время отклика — быстрое, секунды; производительность — малая или средняя;
- требования безопасности и надежности — высокие;
- вычислительная система и среда — микропроцессорное управление и системы реального времени;
- требования к вычислительным ресурсам — высокие, почти полное использование ресурсов по основному функциональному назначению.

Требования функциональной безопасности относятся к достаточно узкому классу базовых и прикладных программных средств, которому соответствуют около 10 — 15% от общего числа типов характеристик, перечисленных в стандарте. Такие ПС применяются при управлении: движущимися объектами на транспорте и в авиации, в атомной энергетике, в автоматизированных производствах, во встроенных компьютерных системах и программируемых электронных системах безопасности (см. **IEC 61508**, **IEC 60880**). Характеристики и особенности выделенных типов ПС, для которых имеет важнейшее значение функциональная безопасность, могут быть несколько расширены свойствами комплексов программ информационных систем, в которых доминирующее значение имеет информационная безопасность, но отражающаяся на функциональной безопасности.

Однако далее учитываются базовые и прикладные ПС, преимущественно с перечисленными выше характеристиками. При этом предполагается, что функции обеспечения функциональной безопасности могут реализоваться автономными программами или органически входить в основные комплексы функциональных программ управления системой или процессами. Применение основных характеристик ПС в стандарте **ISO 12182** иллюстрировано таблицей связей с характеристиками

качества комплексов программ, представленными в стандарте **ISO 9126**, и несколькими примерами.

Общее представление о **характеристиках качества программных средств** международным стандартом **ISO 9126** рекомендуется отражать тремя взаимодействующими и взаимозависимыми **метриками характеристик качества**, описывающими:

- внутреннее качество, проявляющееся в процессах разработки, модификации и других промежуточных этапах жизненного цикла ПС;
- внешнее качество, заданное требованиями заказчика в спецификациях и отражающееся характеристиками конечного продукта;
- качество при использовании в процессе нормальной эксплуатации и результативностью достижения потребностей пользователей с учетом затрат ресурсов.

Эти типы метрик применимы при определении целей системы и требований к ПС, включая промежуточные компоненты и продукты. Подходящие внутренние атрибуты качества ПС являются предпосылкой достижения в жизненном цикле требуемого внешнего поведения, а приемлемое внешнее поведение — предпосылка достижения качества в использовании.

Стандартами рекомендуется, чтобы было предусмотрено **измерение или оценивание каждой характеристики ПС** (субхарактеристики или ее атрибута) с точностью и определенностью, достаточной для сравнений с требованиями технических заданий и спецификаций, и чтобы измерения были объективны и воспроизводимы. Следует предусматривать нормы допустимых ошибок измерения, вызванных инструментами и/или ошибками человека-эксперта. Чтобы измерения были объективными, должна быть документирована и согласована процедура для присвоения числового значения, свойства или категории каждому атрибуту программного продукта. Процедуры измерений должны давать в результате одинаковые меры с приемлемой устойчивостью, получаемые различными субъектами при выполнении одних и тех же оцениваний характеристик ПС.

Характеристики, субхарактеристики и атрибуты качества ПС с позиции возможности и точности их измерения можно разделить на **три уровня детализации показателей**, особенности которых следует уточнять при их выборе:

- категорийные-описательные, отражающие набор свойств и общие характеристики объекта — его функции, категории ответственности, безопасности и важности, которые могут быть представлены номинальной шкалой — категорий-свойств;
- количественные — представляемые множеством упорядоченных числовых точек, отражающих непрерывные или дискретные закономерности и описываемые интервальной или относительной шкалой, которые можно объективно измерить и численно сопоставить с требованиями;
- качественные — содержащие несколько упорядоченных или отдельных свойств — категорий, которые характеризуются порядковой или точечной шкалой набора категорий (есть — нет, хорошо — плохо), устанавливаются, выбираются и оцениваются в значительной степени субъективно и экспертно.

К **первому уровню** относятся показатели качества, которые характеризуются наибольшим разнообразием значений — свойств программ и наборов данных и охватывают весь спектр классов, назначений и функций современных ПС. Эти свойства можно сравнивать только в пределах однотипных ПС и трудно упорядочивать по принципу предпочтительности. Среди стандартизированных показателей качества к этой группе, прежде всего, относится **Функциональная пригодность**, являющаяся самой важной и доминирующей характеристикой любых ПС. Номенклатура и значения всех остальных показателей качества непосредственно определяются требуемыми функциями программного средства и, в той или иной степени, влияют на выполнение этих функций. Поэтому выбор функциональной пригодности ПС, подробное и корректное описание ее свойств являются **основными исходными данными** для установления при проектировании **требуемых значений функциональной безопасности** и всех остальных стандартизированных показателей качества.

Ко **второму уровню** показателей качества относятся достаточно достоверно и объективно измеряемые численные характеристики ПС. Значения этих конструктивных характеристик обычно в наибольшей степени влияют на функциональную пригодность и метрики в использовании ПС. Поэтому выбор и обоснование их требуемых значений должно проводиться наиболее достоверно уже при проектировании ПС. Их субхарактеристики могут быть описаны упорядоченными шкалами объективно измеряемых значений, требуемые численные величины которых могут быть установлены и выбраны заказчиками или пользователями ПС. Такими характеристиками являются корректность, функциональная безопасность, надежность и эффективность комплексов программ. Эти величины могут выбираться и фиксироваться в техническом задании или спецификации требований и сопро-

вождаться методикой объективных, численных измерений при квалификационных испытаниях для сопоставления с требованиями.

Третий уровень стандартизированных показателей качества ПС трудно полностью описать измеряемыми количественными значениями и их некоторые субхарактеристики и атрибуты имеют описательный, качественный вид. В зависимости от функционального назначения ПС по согласованию с заказчиком можно определять экспертно степень необходимости (приоритет) этих свойств и бальные значения уровня реализации их атрибутов в жизненном цикле конкретного ПС.

Различия между ожидаемыми и полученными результатами функционирования программ могут быть следствием ошибок не только в созданных программах и данных, но и **системных ошибок в первичных требованиях спецификаций**, явившихся исходной базой при создании ПС. Тем самым проявляется объективная реальность, заключающаяся в невозможности абсолютной корректности исходных спецификаций требований сложных ПС для проектирования. На практике в процессе разработки ПС исходные требования уточняются и детализируются по согласованию между заказчиком и разработчиком. Базой таких уточнений являются неформализованные представления и знания специалистов, а также результаты промежуточных этапов жизненного цикла. Однако установить ошибочность исходных данных и спецификаций еще труднее, чем обнаружить ошибки в созданных программах, так как принципиально отсутствуют формализованные данные, которые можно использовать как эталонные, и их заменяют неформализованные представления заказчиков и разработчиков.

Дефекты функционирования программных средств, не имеющие злоумышленных источников или последствий физических разрушений аппаратных компонентов, проявляются внешне как случайные, имеют разную природу и последствия. Полное устранение негативных воздействий и дефектов, отражающихся на безопасности и качестве функционирования сложных ПС, принципиально невозможно. Проблема состоит в выявлении факторов, от которых они зависят, в создании методов и средств уменьшения их влияния на функциональную пригодность ПС, а также в эффективном распределении ограниченных ресурсов для обеспечения необходимого качества функционирования комплекса программ, равнопрочного при всех реальных негативных воздействиях. Комплексное, скоординированное применение этих методов и средств в процессе создания, развития и применения ПС позволяет исключать проявления ряда негативных факторов или значительно ослаблять их влияние. Тем самым уровень достигаемой **функциональной безопасности и качества функционирования ПС может быть предсказуемым и управляемым**, непосредственно зависящим от ресурсов, выделяемых на его достижение, а главное, от системы качества и эффективности технологий, используемых на всех этапах жизненного цикла ПС.

Для выбора при проектировании значений характеристик качества программных средств необходимо, прежде всего, установить диапазоны рациональные мер и шкал для каждой субхарактеристики и ее атрибутов, которые целесообразно использовать в качестве **первичных ограничений** их значений для реальных ПС. Далее должны быть разработаны процессы определения и представления в спецификациях проекта, требований к свойствам и атрибутам каждой характеристики качества. Эти требования должны учитывать реальные ограничения ресурсов, доступных для их достижения в ЖЦ ПС [7, 10, 14].

Решение этих задач должно быть направлено на обеспечение высокой функциональной пригодности ПС **путем сбалансированного улучшения безопасности и остальных характеристик качества в условиях ограниченных ресурсов на ЖЦ**. Для этого в процессе системного анализа при подготовке технического задания и требований спецификаций, значения атрибутов и характеристик безопасности и качества должны выбираться с учетом их влияния на функциональную пригодность. Излишне высокие требования к отдельным атрибутам качества, требующие для реализации больших дополнительных трудовых и вычислительных ресурсов, целесообразно снижать, если они слабо влияют на основные, функциональные характеристики ПС. Ориентирами могут служить диапазоны изменения атрибутов конструктивных характеристик качества ПС, границы количественных или качественных шкал которых сверху и снизу могут быть выбраны **на основе следующих принципов**:

- предельные значения характеристик функциональной безопасности и качества должны быть ограничены сверху допустимыми или рациональными затратами ресурсов на их достижение при разработке и совершенствовании системы и ПС;
- наибольшие допустимые затраты ресурсов, например, труда и времени, для реализации функциональной безопасности и конструктивных характеристик должны обеспечивать функциональную пригодность жизненного цикла системы и ПС на достаточно высоком уровне;
- допустимые наихудшие значения безопасности и отдельных конструктивных характерис-

тик качества могут соответствовать значениям, при которых начинает снижаться функциональная пригодность при применении системы и ПС;
- ограниченные значения отдельных конструктивных характеристик качества не должны негативно отражаться на возможных высоких значениях других приоритетных характеристик.

Функциональная пригодность — наиболее ответственная, неопределенная, объективно трудно формализуемая и оцениваемая в проектах характеристика комплексов программ, которая значительно определяет требования к обеспечению функциональной безопасности системы и ПС. Области применения, номенклатура и функции комплексов программ охватывают столь разнообразные сферы деятельности человека, что невозможно полностью выделить и унифицировать достаточно ограниченное число атрибутов для выбора и сравнения этой характеристики у различных по назначению комплексов программ. Перед системным проектированием комплекса программ заказчиком должен описываться **исходный набор свойств ПС** (см. **ISO 12182**), которые в дальнейшем используются в качестве эталонов при формализации функциональной пригодности.

Функциональная пригодность — это набор и описания атрибутов, определяющих **назначение, основные, необходимые и достаточные функции ПС**, заданные техническим заданием и спецификациями требований заказчика или потенциального пользователя. В процессе проектирования комплекса программ атрибуты функциональной пригодности должны конкретизироваться в спецификациях на ПС в целом и на компоненты. Атрибутами этой характеристики качества могут быть функциональная полнота решения заданного комплекса задач, степень покрытия функциональных требований спецификациями и их стабильность при совершенствовании ПС, число реализуемых требований заказчиков и т.д. Кроме них функциональную пригодность отражают множество различных специализированных критериев, которые тесно связаны с конкретными решаемыми задачами и сферой применения комплекса программ. Их можно рассматривать как частные критерии или как факторы, влияющие на основной показатель качества ПС.

Эта характеристика может значительно модифицироваться в жизненном цикле ПС и соответственно изменять конкретное содержание функций, которые подлежат применению и оцениванию. На последовательных этапах ЖЦ функции промежуточных продуктов (спецификаций компонентов, модулей, текстов программ и т.п.) должны оцениваться на соответствие описаниям в отдельных, частных документах. Это позволяет поэтапно формализовать применяемые субхарактеристики и атрибуты функциональной пригодности. Такими атрибутами могут быть: функциональная адекватность программ документам и декларированным требованиям, утвержденным заказчиком; степень покрытия тестами исходных требований; полнота и законченность реализации этих требований; точность выполнения требований детальных спецификаций на функциональные компоненты ПС.

Среди всего многообразия функциональных характеристик программных средств можно выделить **две группы**, одна из которых отражает разнообразные специфические особенности, связанные непосредственно с назначением, функциями и сферой применения ПС, а вторая — доступна для частичной унификации состава и структуры, а также для оценивания стандартизированными методами. Эта вторая группа характеризует **ряд базовых, инвариантных свойств качества**, которые позволяют определять некоторые субхарактеристики функциональной пригодности ПС при разных конкретных целях и сферах применения. С этой позиции функциональная пригодность определяется качеством взаимосвязи и согласованности последовательных формулировок содержания и реализации основных фрагментов в цепочке стандартизированных требований технического задания на ПС: **целей – назначения – функций – исходной информации – результатов для пользователей**, определяющих, что:
- описание целей программного средства корректно переработано в подробное описание его назначения и внешней среды применения;
- назначение ПС полностью и корректно детализировано в требованиях к функциям комплекса программ и его компонентов;
- реализация требований к функциям ПС обеспечена достоверным и адекватным составом и содержанием исходной информации и свойств объектов внешней среды;
- реализация функций ПС способна подготавливать всю требуемую и достаточно корректную информацию для пользователей и объектов внешней среды.

Цель жизненного цикла или **системная эффективность** ПС может оцениваться, в основном, экспертно и является исходной для прослеживания всех последующих, производных свойств и атрибутов функциональной пригодности. Назначение ПС детализируются и формализуются в **требованиях к функциям** компонентов и всего комплекса программ, способного реализовать декларированные

цели. Адекватность и полнота отражения требуемыми функциями сформулированного назначения ПС являются характеристикой, определяющей потенциальную возможность реализации его функциональной пригодности в целом. Прослеживание детализации и покрытия целей требованиями к функциям сверху вниз (начиная от целей системы), а также конкретизация и корректировка целей снизу вверх от потенциально реализуемых функций должны обеспечивать адекватность и качество этой части декларируемой основы функциональной пригодности.

Функции программного средства реализуются в определенной аппаратной, операционной и пользовательской внешней среде системы, характеристики которой существенно влияют на функциональную пригодность. Для выполнения требуемых функций комплекса программ необходима **адекватная исходная информация от объектов внешней среды**, содержание которой должно полностью обеспечивать реализацию декларированных функций. Полнота формализации номенклатуры, структуры и качества входной информации для выполнения требуемых функций, является одной из важных составляющих при определении функциональной пригодности ПС в соответствующей внешней среде.

Цель и функции ПС реализуются тогда, когда **выходная информация** достигает потребителей — объектов или операторов-пользователей с требуемым содержанием и качеством, достаточным для обеспечения её эффективного применения. Содержательная часть этой информации определяется конкретными задачами системы, их основными технико-экономическими и/или социальными показателями функционирования и отражается метриками в использовании. **Степень покрытия** всей выходной информацией: целей, назначения и функций ПС для пользователей, следует рассматривать как **основную меру качества функциональной пригодности**. Прослеживание и оценивание адекватности и полноты состава выходной информации снизу вверх к назначению ПС должны завершать выбор базовых субхарактеристик качества функциональной пригодности, независимо от сферы применения системы.

В процессе проектирования в составе функциональной пригодности могут быть выделены две группы базовых субхарактеристик, определяющие функциональные и структурные требования и особенности ПС. При формализации и выборе **функциональных требований** следует возможно четко **формулировать в документах контракта**:

- экономические, организационные, технические и/или социальные стратегические цели всего жизненного цикла системы, ПС и его компонентов;
- системную эффективность и, в том числе, требуемые технико-экономические показатели применения ПС в составе системы;
- назначение, внешнюю среду, условия эффективного и безопасного применения ПС;
- функциональные задачи основных компонентов и ПС в целом, а также системную эффективность каждого компонента;
- необходимую и достаточную безопасность применения, характеристики качества и временной регламент решения каждой функциональной задачи;
- соответствие ПС и его компонентов выделенным стандартам и нормативным документам на проектирование и применение.

В зависимости от назначения ПС функциональная безопасность и/или некоторая конструктивная характеристика может стать доминирующей или даже почти полностью определяющей функциональную пригодность ПС. В наибольшей степени функциональная пригодность во многих случаях зависит от **функциональной безопасности, корректности и надежности ПС**. Эти характеристики трудно свести к количественным мерам и зачастую их приходится оценивать по наличию свойств и ряда типовых процедур в ПС или по величине необходимых затрат ресурсов, достаточно заметно влияющих на функциональную пригодность.

Правильность – корректность: это способность ПС обеспечивать правильные или приемлемые по качеству результаты для пользователей. Эталонами для выбора требований к корректности при проектировании могут быть: верифицированные и взаимоувязанные требования к функциям комплекса, компонентов и модулей программ, а также правила их структурного построения, организация взаимодействия и интерфейсов. Эти требования к ПС при разработке должны быть прослежены сверху вниз до модулей и использоваться как эталоны при установлении необходимой корректности соответствующих компонентов. Данное понятие включает обеспечение эталонных (ожидаемых) данных с необходимой степенью точности расчетных значений в соответствии с требованиями технического задания и спецификаций. В процессе проектирования и разработки модулей и групп программ применяются частные структурные критерии корректности, которые включают корректность структуры программ, обработки данных и межмодульных интерфейсов. Каждый из частных критериев может характеризоваться несколькими методами измерения качества и достигаемой степенью корректности

программ: детерминировано, стохастически или в реальном времени.

Требования к характеристике **корректность** могут представляться в виде описания двух основных свойств, которым должны соответствовать все программные компоненты и ПС в целом. Первое требование состоит в выполнении определенной степени (%) прослеживаемости и верификации сверху вниз реализации требований технического задания и спецификации на ПС при последовательной детализации описаний программных компонентов вплоть до текстов и объектного кода программ.

Второе требование заключается в выборе степени и стратегии покрытия тестами структуры и функций программных компонентов, совокупности маршрутов исполнения модулей и всего комплекса программ для последующего процесса верификации и тестирования, достаточного для функционирования ПС с необходимым качеством и точностью результатов при реальных ограничениях ресурсов. Для определения этой величины при разработке ПС необходима организация регулярной регистрации, накопления имен, содержания функций и маршрутов исполнения программ, прошедших тестирование, а также контроль доли не тестированных от всей совокупности. Мерой выбранной корректности может быть относительное число протестированных функций и маршрутов, которое может измеряться в процентах от общего числа исполняемых. Опыт показывает, что зачастую в готовом, сложном ПС оказываются протестированными только около 50-70% функций и маршрутов, и практически очень трудно эту величину довести до 90-95%. Косвенно эту величину при определенной автоматизации и квалификации специалистов отражает трудоемкость и длительность тестирования, что непосредственно влияет на функциональную пригодность ПС.

4. Ресурсы для обеспечения функциональной безопасности программных средств

Многие проекты обеспечения безопасности систем терпели и терпят неудачу из-за отсутствия у разработчиков и заказчиков при подготовке контракта четкого представления о реальных финансовых, трудовых, временных и иных ресурсах, необходимых и доступных для их реализации. Поэтому одной из основных задач при проектировании функциональной безопасности ПС является **экономический анализ и определение необходимых ресурсов для создания и всего ЖЦ ПС** в соответствии с требованиями контракта и технического задания [2, 5, 10].

При планировании проектов ПС часто инициатором разработки является разработчик-поставщик, который самостоятельно принимает все решения о проектировании за счет собственных ресурсов и предполагает возместить затраты при реализации ПС на рынке. В других случаях имеется определенный заказчик-потребитель, который способен задать основные цели, характеристики качества и безопасности и обеспечить ресурсы для реализации проекта. Таким образом, **при экономическом обосновании проектов ПС и их функциональной безопасности возможны два сценария**:

- создание и весь жизненный цикл комплекса программ и/или базы данных ориентируется разработчиком на массовое тиражирование и распространение на рынке для заранее неизвестных покупателей-пользователей в различных сферах применения, при этом отсутствует приоритетный внешний потребитель-заказчик, который определяет и диктует основные требования к ПС и его безопасности, а также финансирует проект;
- разработка проекта ПС и/или БД и их безопасности предполагается поставщиком-разработчиком для конкретного потребителя-заказчика, задающего все требования, который его финансирует, с определенным, необходимым ему тиражом и известной ограниченной областью применения результатов разработки.

Первый сценарий базируется на маркетинговых исследованиях рынка программных продуктов и на стремлении поставщика занять на рынке достаточно выгодное место, обеспечивающее ему необходимую прибыль. Важнейшим **фактором конкурентоспособности ПС является соотношение между ценностью (эффективностью)** имеющегося или предполагаемого продукта с позиции его использования потребителем и стоимостью его при создании или приобретении в условиях реального рынка. Для этого нужно определить наличие на рынке гаммы близких по назначению ПС, оценить их экономическую эффективность, стоимость, применяемость и безопасность, а также возможную конкурентоспособность предполагаемого программного продукта для потенциальных пользователей и их возможное число. Кроме того, следует оценить рентабельность затрат на обеспечение всего ЖЦ нового ПС и выявить функциональные и конструктивные характеристики качества и безо-

пасности, которые способны привлечь достаточно покупателей и оправдать затраты на предстоящую разработку.

Второй сценарий предполагает наличие определенного заказчика-потребителя проекта ПС, который определяет основные технические и экономические требования и функциональные характеристики. Он выбирает конкурентоспособного поставщика-разработчика, которого оценивает на возможность реализовать проект с необходимым качеством и функциональной безопасностью с учетом ограничения сроков, бюджета и других ресурсов. Этому помогает опыт и экономические характеристики ранее выполненных поставщиками проектов, но некоторые проекты могут не иметь явных прецедентов, и тогда приходится использовать имеющуюся статистику в этой области. При этом предполагается, что результаты разработки могут не поступать на открытый рынок, вследствие чего маркетинговые исследования для таких проектов не являются доминирующими и обычно предварительно могут не проводиться.

При прогнозировании необходимых ресурсов для проекта, ЖЦ ПС и обеспечение его безопасности можно разделить на две части, существенно различающиеся экономическими особенностями процессов, характеристиками и влияющими на них факторами. **В первой части ЖЦ** производятся системный анализ, проектирование, разработка, тестирование и испытания базовой версии ПС. Номенклатура работ, их трудоемкость, длительность и другие экономические характеристики на этих этапах ЖЦ существенно зависят от требуемых характеристик системы и ее безопасности, технологии и инструментальной среды разработки.

Вторая часть ЖЦ ПС, отражающая эксплуатацию, сопровождение, модификацию и перенос ПС на иные платформы, в меньшей степени связана с функциональными характеристиками системы и среды разработки. Номенклатура работ на этих этапах более или менее определенная и стандартизированная (см. **ISO 12207**, **ISO 14764**, **ISO 15846**), но их трудоемкость и длительность могут сильно варьироваться в зависимости от массовости и других внешних факторов распространения и применения версий ПС. Определяющими становятся потребительские характеристики ПС, а их экономические особенности с позиции разработчиков и вложенные затраты на очередную версию отходят на второй план (см. первый сценарий). Поэтому планы на этих этапах имеют характер общих взаимосвязей содержания работ, которые требуют распределения во времени индивидуально для каждого проекта.

Важнейшим ресурсом при создании любых ПС являются люди — **специалисты** с их уровнем профессиональной квалификации, а также с многообразием знаний, опыта, стимулов и потребностей. Быстрый рост сложности и повышение ответственности за качество и функциональную безопасность комплексов программ привели к появлению **новых требований к специалистам**, обеспечивающим все этапы жизненного цикла ПС. Эти специалисты должны владеть новой интеллектуальной профессией, обеспечивающей высокое качество и безопасность ЖЦ ПС, а также контроль, испытания и удостоверение реального достигнутого качества на каждом этапе разработки и совершенствования программ.

Безопасность вычислительной системы с ПС обеспечивается двумя видами работ: созданием функциональных программ высокого качества с минимальным количеством дефектов и ошибок, отражающихся на безопасности, и разработкой специального комплекса программ, повышающих безопасность функционирования основных программ. **Руководство безопасностью сложного проекта ПС** должны осуществлять лидеры — менеджеры:

- **менеджер безопасности проекта** — это специалист, обеспечивающий коммуникацию между заказчиком и проектной командой специалистов, его задача — определить и обеспечить полное удовлетворение требований заказчика по безопасности системы и ПС;
- **менеджер-архитектор комплекса программ повышения безопасности** — управляет коммуникациями и взаимоотношениями в проектной команде, является координатором создания компонентов, разрабатывает базовые, функциональные спецификации и управляет ими, ведет график проекта и отчитывается за его состояние, инициирует принятие критичных для хода проекта решений.

Функции специалистов и технология работы при обеспечении ЖЦ комплекса программ повышения безопасности ПС аналогичны тем, которые применяются при создании основных компонентов, определяющих функциональную пригодность ПС и системы. В реализации любого крупного проекта ПС можно выделить две категории специалистов: разрабатывающих компоненты и ПС в целом и обеспечивающие технологию, безопасность и качество программного продукта. При выборе заказчиком надежного поставщика-разработчика проекта необходима **оценка тематической и технологической квалификации** возможного коллектива специалистов, а также его способности реализо-

вать проект с заданными требованиями, качеством и функциональной безопасностью.

Специалисты первой категории непосредственно создают компоненты и ПС в целом с заданными показателями качества и безопасности. В процессе разработки их функции заключаются в тщательном соблюдении принятой в фирме технологии и в формировании всех предписанных руководствами исходных и отчетных документов. Разделение труда специалистов этой категории в крупных проектных коллективах приводит к необходимости их дифференциации по квалификации и областям деятельности:

- **спецификаторы** — подготавливают описания функций соответствующих компонентов с уровнем детализации, достаточным для корректной разработки текстов программ программистами;
- **разработчики программных компонентов (программисты)** создают компоненты, удовлетворяющие спецификациям, реализуют требуемые функции продукта;
- **системные интеграторы** создают на выходе требуемые крупные компоненты или комплекс программ;
- **тестировщики** — обеспечивают проверку функциональных спецификаций, выполняют тестирование для каждой из фаз и компонента проекта;
- **управляющие сопровождением и конфигурацией** — обеспечивают взаимодействие компонентов и реализацию версий ПС;
- **документаторы** — осуществляют подготовку и издание сводных технологических и эксплуатационных документов в соответствие с требованиями стандартов.

Специалисты второй категории — технологи, обслуживающие и сопровождающие технологический инструментарий, который применяется специалистами первой категории, обеспечивают применение системы качества проекта или предприятия, контролируют и инспектируют ее использование. Специалисты, управляющие обеспечением качества и безопасности ПС, должны овладеть стандартами и методиками фирмы, поддерживающими регистрацию, контроль, документирование и воздействия на показатели качества на всех этапах ЖЦ программ. Они должны обеспечивать эксплуатацию системы качества проекта, выявление всех отклонений от заданных показателей качества и безопасности объектов и процессов, а также от предписанной технологии на промежуточных и заключительных этапах разработки.

Для **анализа затрат ресурсов в жизненном цикле ПС** их целесообразно разделить на две части (рис. 4):

- затраты на создание программных компонентов, обеспечивающих **базовые свойства функциональной пригодности** комплекса программ для его применения по прямому назначению пользователями в соответствии с требованиями контракта и технического задания;
- основные составляющие **дополнительных затрат**, обеспечивающие требуемые конструктивные характеристики качества и безопасности для улучшения функциональной пригодности ПС в соответствии с целями и сферой его применения.

Обеспечение функциональной пригодности является основной целью при использовании финансовых, трудовых, вычислительных и других ресурсов в жизненном цикле ПС. Эти затраты зависят, в первом приближении, от сложности алгоритмов, объема комплекса программ и баз данных, которые определяют трудоемкость и длительность полного цикла их разработки. Основные затраты идут на овеществленный, преимущественно интеллектуальный труд специалистов различных категорий. Поэтому для их измерения наиболее универсальной единицей стали трудозатраты специалистов в человеко-днях или человеко-месяцах, которые обычно достаточно просто могут преобразовываться в стоимость процесса разработки [2, 6, 10]. Однако это не значит, что затраты на решение этой основной задачи всегда являются доминирующими по величине. Необходимость выполнения ряда требований к остальным конструктивным характеристикам качества и безопасности часто приводит к тому, что использование ресурсов на их реализацию может превышать базовые затраты на обеспечение функциональной пригодности. В то же время затраты на выполнение этих требований всегда направлены на повышение и совершенствование функциональной пригодности.

Абсолютная величина затрат на разработку ПС, также как и ее длительность, зависят от ряда факторов, которые могут изменять их в различных направлениях. При анализе **затрат на обеспечение требуемых функций** сложных ПС доминирующим фактором, влияющим на их величину, является сложность функциональной части комплекса программ и базы данных. Наиболее активно в качестве простейшего показателя сложности используется **объем программ, выраженный числом** операторов (команд) или строк текста на языке программирования (с учетом коэффициента, зависящего от класса ПС и специфики языка). Объем программ,

без комментариев, является одной из наиболее достоверно измеряемых характеристик сложности ПС и достаточно адекватен экономическим затратам на его разработку. Реальное изменение создаваемых в настоящее время **новых сложных ПС** объемом от 10^3 до 10^6 строк определяет диапазон трудоемкости разработки таких программ от человеко-года до тысяч человеко-лет.

Ограниченные ресурсы времени реализации проектов ПС являются одним из самых **сильных факторов**, влияющих на достижимое качество и безопасность комплексов программ. При реальном допустимом времени реализации проекта оно ограничивает затраты на все промежуточные этапы работ и тем самым на качество их выполнения. При современных технологиях полностью новые, сложные комплексы программ, реализуемые в допустимое время 2—4 года, ограничены объемом $10^6 — 10^7$ строк текста. Очевидна принципиальная нерентабельность разработки очень сложных ПС за 5—10 лет. С другой стороны, даже относительно небольшие программы высокого качества в несколько тысяч строк по полному технологическому циклу с сертификационными испытаниями продукции редко создаются за время, меньшее, чем полгода — год. Таким образом, диапазон вариации длительностей разработок ПС много меньше, чем вариация их трудоемкости, а эти длительности ограничены сверху и снизу, и объем новых программ является одним из основных факторов, определяющим эти границы.

Любые ПС должны поступать на эксплуатацию, сохраняя актуальность до того, как в них пропадает необходимость. Их цели, концептуальная основа и алгоритмы не должны устареть за время разработки. Отсюда появляется **верхний предел** допустимых длительностей разработки. Стремление заказчиков ограничивать длительность реальных разработок ПС приводит к объективному формированию ее верхнего предела (2 — 4 года), зависящего в основном от объема и класса ПС, за которым распространяется зона «нерациональных» длительностей.

Границу длительностей снизу определяют естественный технологический процесс коллективной разработки и необходимость выполнения ряда взаимоувязанных работ на последовательных этапах, которые обеспечивают получение сложных ПС требуемого качества. Подготовка текстов программ, их тестирование, комплексирование, документирование и испытания могут проводиться в основном последовательно, и каждый этап требует некоторого времени. Под воздействием перечисленных факторов формируется объективный минимум возможных длительностей разработок —

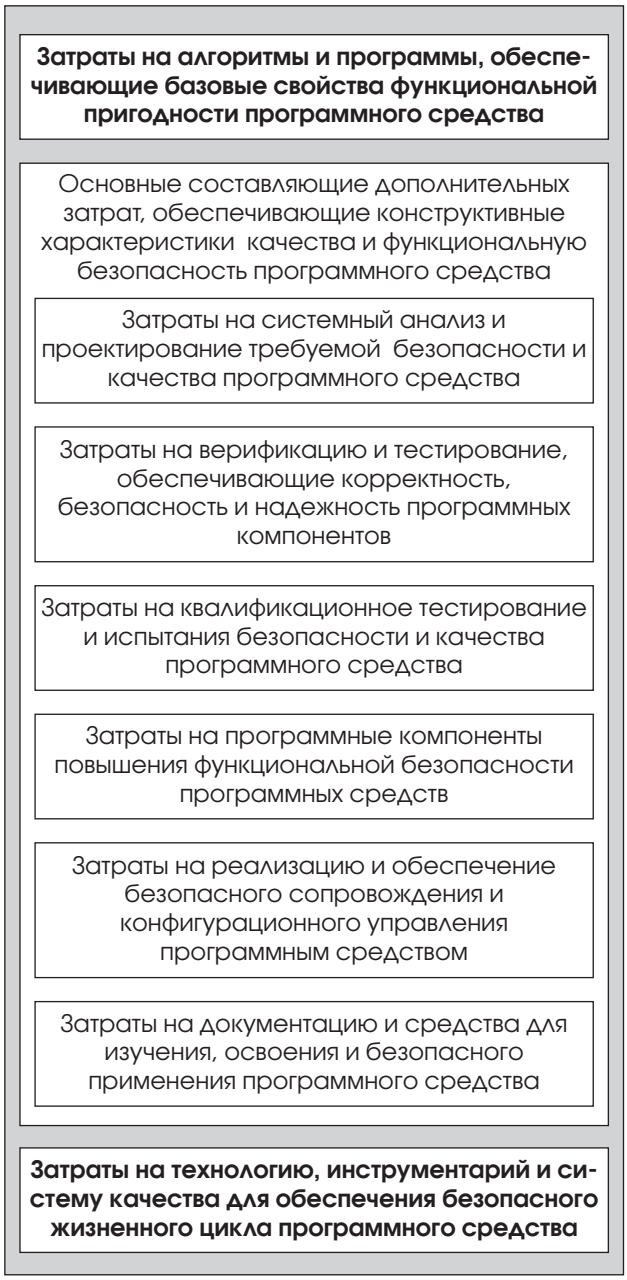

Рис. 4

граница снизу области «невозможных» длительностей, зависящая в первую очередь от объема разрабатываемых ПС. Эта граница может варьироваться в небольших пределах (1 — 2 года для сложных ПС) за счет: совершенствования технологии, повышения программной и аппаратурной оснащенности разработки, а также вследствие роста коллективной квалификации разработчиков и заказчиков.

Основные составляющие **дополнительных затрат**, обеспечивающих требуемые характеристики функциональной безопасности и качества ПС, целесообразно структурировать в соответствии с их номенклатурой в стандарте **ISO 9126**. Эти затраты обычно состоят из двух связанных частей: из **затрат на реализацию** соответствующих характерис-

тик качества в программных продуктах и из **затрат при использовании** этих характеристик в процессе эксплуатации комплекса программ. Важнейшее значение имеет установление и формализация исходных требований к характеристикам качества и безопасности ПС. Поэтому целесообразно выделять ресурсы на системный анализ и проектирование требований ко всему комплексу характеристик безопасности и качества на начальных этапах проекта ПС. Обычно совершенствование качества и повышение затрат на реализацию характеристик способствует снижению затрат при их эксплуатации.

Затраты ресурсов на **обеспечение корректности** зависят от полноты прослеживания реализации требований к ПС сверху вниз, от требований к компонентам вплоть до объектного кода программ и от степени их покрытия тестами. Эти затраты входят непосредственно в процесс разработки и зависят от объема и детальности процессов верификации и тестирования. Для сложных ПС при требовании их высокой корректности они могут составлять до 30% от затрат на обеспечение базовой, функциональной пригодности. Для относительно простых комплексов программ эта величина в среднем составляет 10—20%. Эти затраты приходятся на **верификацию и тестирование программных компонентов**, что должно обеспечивать корректность, безопасность ПС и надежность в целом. Хотя эти характеристики различаются, затраты на их реализацию полностью разделить невозможно. Поэтому оценивание и выделение ресурсов на решение этих задач целесообразно анализировать совместно.

Затраты на квалификационное тестирование и испытания ПС в целом обычно могут быть достаточно четко выделены из остальных затрат, так как в этих процессах непосредственно участвуют заказчик и пользователи. Величина этих затрат без учета ресурсов, необходимых для имитации внешней среды, может составлять около 10% от общих затрат на разработку. При этом практически невозможно разделять затраты на оценивание отдельных стандартизированных характеристик.

Затраты на функциональную безопасность и надежность ПС определяются требуемым уровнем защищенности и сложностью (объемом) программ для ее реализации. При наличии особенно высоких требований к безопасности критических ПС эти затраты могут даже в 2 — 3 раза превышать затраты на решение базовых, функциональных задач. Для типовых систем трудоемкость создания программных средств функциональной безопасности обычно составляет 20 — 40% затрат на решение основных, функциональных задач при требованиях наработки на отказ в десятки тысяч часов и для минимального обеспечения автоматического рестарта в системах.

Возможные затраты трудовых и временных ресурсов **на развитие и совершенствование качества и безопасности комплекса программ** в процессе сопровождения зависят не только от внутренних свойств программ, но также от запросов и потребностей пользователей на новые функции и от готовности заказчика и разработчика удовлетворить эти потребности. Величина этих затрат определяется рыночной конъюнктурой для данного программного продукта и коммерческой целесообразностью его модификации и развития. По объему предполагаемых изменений, а также вновь вводимых в очередную версию компонентов, с учетом сложности и новизны их разработки могут быть оценены затраты на их создание.

Затраты на обеспечение и реализацию сопровождения программ определяются длительностью цикла жизни комплекса программ, его мобильностью, уровнем автоматизации технологии разработки и тиражом программ. Для их оценивания, прежде всего, необходимо выделять основные виды затрат при сопровождении конкретного комплекса программ и наиболее существенные факторы, которые на них влияют. Сокращение затрат на сопровождение возможно за счет некоторого увеличения затрат при разработке ПС, так что при рациональном проектировании в сумме затраты могут быть уменьшены иногда весьма заметно. Затраты на сопровождение можно считать аддитивными и включающими **составляющие**:

- затраты на обнаружение и устранение ошибок и дефектов в каждой версии ПС;
- затраты на доработку и совершенствование программ, формирование и испытание новых модернизированных версий ПС;
- затраты на тиражирование каждой новой версии и ее внедрение в эксплуатируемых и новых ПС.

В современных проектах ПС большую или меньшую долю составляют **готовые апробированные компоненты** из других подобных разработок — **прототипы и/или покупные пакеты прикладных программ**. Это позволяет значительно ускорять работы и сокращать затраты на создание сложных комплексов программ. Перед разработчиками проекта ПС зачастую возникает дилемма: разрабатывать ли весь комплекс программ (в том числе для обеспечения безопасности) полностью из новых компонентов или использовать, адаптировать и приспосабливать готовые компоненты (какие и в каком количестве). В результате при пер-

вичном экономическом анализе затрат на создание ПС с требуемыми характеристиками безопасности целесообразно рассматривать **два альтернативных варианта** определения затрат на разработку:

- полностью нового ПС, для которого отсутствуют или недоступны подходящие готовые компоненты — прототипы и/или их заведомо нерентабельно использовать;
- программного средства на базе комплексирования набора готовых программных компонентов и информации баз данных, для которого почти не требуется создания новых компонентов.

При сборке нового ПС из комплектующих компонентов может потребоваться доработка некоторых из них или создание специальных программ для их взаимодействия. В пределе при построении нового ПС на 80—90% из готовых компонентов суммарные затраты могут сокращаться в 3—5 раз. В этом случае кроме 10—20% затрат на создание новых программных компонентов, необходимы ресурсы на комплексирование нового ПС, его квалификационное тестирование, испытания и документирование.

При создании сложных ПС одной из больших составляющих затрат могут быть **ресурсы на генерацию тестов**. В ряде случаев они соизмеримы с затратами на создание основных функций комплексов программ (в том числе для обеспечения безопасности), что определяется принципиальным соответствием **сложности необходимых наборов тестов** и тестового покрытия программ, и **сложности функций**, реализуемых испытываемым ПС. Создание представительных совокупностей тестов возможно путем использования реальных объектов внешней среды или с помощью программных имитаторов, адекватных этим объектам по результатам функционирования и генерируемой информации. При этом возникает проблема — какой метод и когда выгодней по затратам на генерацию тестов и по обеспечению необходимой степени покрытия тестами испытываемых ПС. Затраты ресурсов на натурные эксперименты для генерации тестов при проведении разработки, испытаний и определения качества пропорциональны реальному времени функционирования проверяемого ПС и затратам на применение привлекаемых средств реальной внешней среды. Они включают стоимость эксплуатации реального объекта, создающего тесты в единицу времени.

Имитаторы тестов необходимы не только для оценивания достигнутых характеристик безопасности и качества комплексов программ, но также для их комплексной отладки, квалификационного тестирования, испытаний при создании версий. Поэтому затраты на программные имитаторы и их экономическую эффективность целесообразно рассматривать с учетом всего комплекса задач, которые они способны и должны решать в ЖЦ ПС. Затраты на программную имитацию тестовых данных определяются ресурсами, необходимыми на проектирование и эксплуатацию сложных комплексов программ для этих целей и следующими **составляющими**:

- затратами на разработку комплекса программ для имитации информации внешних объектов и среды их функционирования;
- затратами на эксплуатацию программ имитации за время проведения тестирования, испытаний и/или определения характеристик безопасности и качества тестируемого ПС;
- затратами на первичную установку и эксплуатацию моделирующей ЭВМ и вспомогательного оборудования, используемого в имитационном стенде.

Затраты на эксплуатацию программ имитации в основном определяются длительностью проведения тестирования, испытаний и/или измерения характеристик безопасности и качества ПС. Значения этого времени соответствуют реальному времени генерации тестовых данных и тестирования программ. Обычно имитаторы используются для тестирования нескольких ПС разного, но близкого целевого назначения. В результате удельные затраты на их создание и эксплуатацию быстро убывают при унификации имитаторов и расширении области их применения для тестирования и оценивания качества большого числа ПС, имеющих близкое функциональное назначение. Даже приближенные оценки этих затрат в большинстве случаев показывают **высокую рентабельность программных имитаторов внешней среды**, особенно для квалификационного тестирования и оценивания характеристик безопасности сложных ПС реального времени.

Литература

1. Безопасность информации. Сборник материалов международной конференции. М.: СИП РИА. 1997.
2. Боэм Б.У. Инженерное проектирование программного обеспечения: Пер. с англ. /Под ред. А.А. Красилова. М.: Радио и связь. 1985.

3. Галатенко В.А. Основы информационной безопасности. Курс лекций. Интернет — Университет Информационных Технологий. М.: ИНТУИТ. 2003.
4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Книга 1 и 2. М.: Энергоатомиздат. 1994.
5. Липаев В.В., Потапов А.И. Оценка затрат на разработку программных средств. М.: Финансы и статистика. 1988.
6. Липаев В.В. Отладка сложных программ. М.: Энергоатомиздат. 1993.
7. Липаев В.В. Методы обеспечение качества крупномасштабных программных средств. М.: СИНТЕГ. 2003.
8. Липаев В.В. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств. М.: Jet Info. № 3 . 2004.
9. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т. и др. Оценка безопасности информационных технологий. Общие критерии. Под ред. В.А. Галатенко. М.: СИП РИА. 2001.
10. Фатрелл Р.Т., Шафер Д.Ф., Шафер Л.И. Управление программными проектами: достижение оптимального качества при минимуме затрат. Пер. с англ. М.: Вильямс. 2003.
11. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. М.: СИНТЕГ. 2000.
12. Encyclopedia of Software Engineering. Vol.1 A-N; Vol.2 O-Z. Editor — In — Chief John J. Marciniak. John Wiley & Sons. Inc. 1995.
13. Musa J.D., Iannino A., Okumoto K. Software Reliability: Measurement, Prediction, Application. N.Y. McGraw Hill. 1987.
14. Sommerville I. Software engineering. Addison — Wesley. Lancaster University. 2000.

Новая книга

Липаев В.В. **Методы обеспечения качества крупномасштабных программных средств.** М.: 2003. 520 с., илл.

Монография состоит из двух частей. **В первой части** рассмотрены основные понятия, факторы и методы представления качества в жизненном цикле (ЖЦ) крупномасштабных программных средств (ПС). Описаны основы базовых стандартов административного управления качеством продукции, процессов жизненного цикла и характеристик качества ПС. Исследована зависимость качества программ от ряда внешних и внутренних факторов, а также от ограниченности ресурсов при создании и применении ПС по прямому назначению. Представлены методы оценки затрат ресурсов на обеспечение функциональной пригодности, на конструктивные характеристики качества, а также на специалистов для обеспечения ЖЦ ПС. Специальный раздел посвящен методам документирования ПС.

Во второй части значительное внимание уделено разработке требований к характеристикам качества ПС, а также планированию процессов ЖЦ и методам проектирования комплексов программ высокого качества. Изложены принципы и методы верификации, технологические этапы и стратегии систематического тестирования ПС, компонентов и обработки потоков данных. Рассмотрены методы стандартизированного оценивания и измерения характеристик качества, которые рекомендуется использовать при подготовке методик испытаний. Представлены методы квалификационного тестирования и испытаний крупномасштабных ПС, оценивания надежности их функционирования и эффективности использования ресурсов ЭВМ. Изложены методы совершенствования качества при сопровождении программ и конфигурационном управлении версиями ПС и компонентов, а также удостоверения достигнутого качества при сертификации программных продуктов.

Монография предназначена для специалистов, обеспечивающих все этапы жизненного цикла крупномасштабных программных средств, создающих и применяющих системы и характеристики качества в этой области. Она может быть полезна исполнителям научных проектов и опытно-конструкторских работ для обеспечения высокого качества сложных программных средств. Ее рекомендуется использовать при обучении студентов и аспирантов созданию сложных комплексов программ.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555