Риски проектирования и производства мобильных программных продуктов

В.В. Липаев
lip@ispras.ru

Аннотация. Вводятся основные понятия и свойства рисков комплексов программ. Рассматриваются факторы и виды рисков комплексов программ и систем. Обсуждается подготовка исходных данных для анализа, прогнозирования и сокращения рисков комплексов программ. Описываются выделение, идентификация, анализ угроз и рисков в комплексах программ. Рассматриваются методы сокращения и ликвидации опасных рисков, регистрации и утверждения допустимого интегрального риска программного продукта.

Ключевые слова: программные продукты, качество и виды рисков программ; дефекты, идентификация, угрозы рисков при производстве и испытаниях программ; регистрация, сокращение и ликвидация рисков программных продуктов.

1. Основные понятия и свойства рисков мобильных комплексов программ

Современные программные продукты для сложных систем активно применяются в критических и ответственных системах динамического управления в ***реальном времени*** объектами, в высокоточном технологическом производстве, в авиации, в управлении космическими аппаратами, атомными электростанциями и оборонной техникой. Они являются одними из наиболее сложных ***интеллектуальных систем высокого качества***, создаваемых человеком и их результатов – программных продуктов [1, 4]. Оценки качества программных продуктов могут проводиться с двух позиций: с ***позиции положительной*** эффективности и адекватности их характеристик назначению, целям создания и применения, а также с ***негативной позиции*** возможного при этом ущерба – риска при их создании и использовании. Характеристики качества и риски объектов и процессов обычно тесно связаны, на них влияют подобные факторы, которые с разных сторон отражаются на свойствах систем или комплексов программ. Показатели качества преимущественно отражают положительный эффект от применения системы или программного продукта и основная задача разработчиков проекта состоит в обеспечении требований

заказчика и пользователей заданного качества. Повышению качества проекта обычно ***сопутствует*** снижение его рисков и наоборот сокращение рисков способствует улучшению характеристик качества. Поэтому методы и системы управления качеством близки к методам анализа и управления рисками комплексов программ, они должны их дополнять и совместно способствовать совершенствованию программных продуктов и систем на их основе.

Риски – это негативные события и их последствия, отражающие потери, убытки или ущерб от процессов или продуктов, вызванные реализацией угроз при наличии уязвимости и ***снижения безопасности*** применения системы. Они проявляются при недостатках и дефектах обоснования, проектирования, производства и всего жизненного цикла комплексов программ. Это негативные последствия функционирования и/или применения программных продуктов, в результате отклонения характеристик объектов или процессов от заданных требований заказчика, согласованных с разработчиками, которые способны нарушать безопасность и вызвать ущерб системе, внешней среде или пользователю [3, 7, 10].

Причинами возникновения и проявления рисков могут быть: ***злоумышленные, активные воздействия заинтересованных лиц*** или ***случайные негативные проявления дефектов*** внешней среды, системы, ошибки разработчиков или пользователей. В первом случае риски могут быть обусловлены искажениями программ и информационных ресурсов и их уязвимостью от предумышленных, внешних воздействий (атак) с целью незаконного использования или искажения информации и программ, которые по своему содержанию предназначены для применения ограниченным кругом лиц. При этом подразумевается наличие лиц, заинтересованных в доступе к конфиденциальной или полезной информации в системах, с целью ее использования или разрушения.

Риски при случайных, дестабилизирующих воздействиях дефектов и отсутствии предумышленного негативного влияния на системы, программный продукт или информацию баз данных зависят от отказовых ситуаций, отрицательно отражающихся на работоспособности и реализации их основных функций. При этом катастрофически, критически или существенно искажается процесс функционирования программного продукта и системы, что может наносить значительный ***ущерб безопасности*** их применения. Одним из косвенных методов определения ***величины риска*** может быть ***оценка совокупных затрат***, необходимых для ликвидации негативных последствий риска в программном продукте, системе или внешней среде, проявляющихся в результате конкретного рискового события.

Анализы рисков – процессы определения источников и количественного оценивания рисков, угроз, уязвимостей, возможного ущерба, а также контрмер для их уменьшения. Для этого предварительно должны быть определены требования к характеристикам комплекса программ и оценки возможного ущерба при их нарушении. Анализ негативного воздействия, должен устанавливать

критерии, используемые для идентификации вторичные последствия, распространяющиеся на компоненты и системы. Модели последствий требуются для прогнозирования размеров возможных аварий, катастроф и других негативных явлений в различных системах. Они включают идентификацию опасностей, угроз и оценки возможных последствий и ущерба от проявления рисков; проверку достоверности результатов анализа рисков; документальное обоснование возможных рисков. В результате анализа следует создавать план ***отслеживания изменения и сокращения рисков в жизненном цикле комплекса программ***, который должен регулярно рассматриваться и корректироваться. [7, 8, 10].

Управление рисками – процесс идентификации, управления, устранения или уменьшения вероятности событий, которые могут негативно воздействовать на комплекс программ, систему и внешнюю среду, действия, осуществляемые для выполнения решений по мониторингу и сокращению рисков. Процесс включает анализ соотношения стоимости/эффективности контрмер, выбор, построение и испытание подсистемы ***обеспечения безопасности***, и исследование всех аспектов проявления рисков системы. Управления рисками предполагает ясное понимание специалистами внутренних и внешних причин и возможных реальных источников угроз, влияющих на качество программного продукта, которые могут привести к большому ущербу.

Анализом и разработкой методов выявления и устранения рисков систем занимается ***Федерация европейской ассоциации менеджеров рисков*** – FERMA. Разработан и опубликован ряд моделей и стандартов, регламентирующих методы анализа и управления рисками проектирования и производства сложных систем. ***Общие методы анализа рисков в сложных системах***, регламентированы стандартами **ISO/IEC 17799, ГОСТ Р 51901,** Семейством международных стандартов Управления информационной безопасностью **ISO 27000,** стандартом **ISO 15408** – Общие критерии оценки безопасности и рисков информационных технологий. Изложенные в стандартах рекомендации могут быть, в частности, применены при анализе и ликвидации рисков сложных комплексов программ и систем [3, 7, 8, 10].

2. Основные факторы и виды рисков комплексов программ и систем

Необходимым требованием к специалистам для выполнения анализа и управления рисками должно быть ***достоверное знание целей и структуры комплекса программ, исследуемой системы и внешней среды***, а также доступных методов анализа и прогнозирования рисков. Область применения методов анализа и сокращения рисков должна быть определена и документально зафиксирована. Для этого следует составить описание основных проблем, определивших целесообразность проведения исследования рисков. Для выработки плана исследований ***область анализа рисков*** должна быть определена и документально установлена. Она должна включать в себя следующее:

- описание оснований и/или проблем, повлекших необходимость анализа рисков, которое включает: формулировку задач анализа рисков, основанных на идентифицированных потенциальных опасностях, угрозах; определении критериев работоспособности и отказов системы;
- описание исследуемой системы – определение границ и областей интерфейса со смежными системами; описание условий окружающей среды;
- установление возможных источников, предоставляющих подробную информацию о всех технических, связанных с окружающей средой, правовых, организационных и человеческих факторах, имеющих отношение к анализируемым действиям и проблеме; обстоятельства, влияющие на безопасность;
- описание используемых предположений и ограничивающих условий при проведении анализа и прогнозировании рисков;
- формулировка возможных решений по сокращению рисков, которые могут быть приняты, описание требуемых выходных данных, полученных по результатам исследований и от лиц, принимающих решения.

Общей задачей анализа риска является обоснование и подготовка решений, касающихся сокращения рисков критических программных продуктов и систем на двух основных стадиях жизненного цикла. ***На стадии проектирования***:

- предоставление исходных данных для оценки качества системы в целом;
- выявление главных возможных источников угроз рисков и предполагаемых факторов, существенно влияющих на риски;
- определение и оценка эффективности возможных мер обеспечения безопасности, закладываемых в программный продукт и систему;
- предоставление исходных данных для оценки потенциально опасных действий, компонентов оборудования или системы;
- обеспечение специалистов соответствующей информацией при проведении опытно-конструкторских работ, ориентированных на нормальные и чрезвычайные условия функционирования комплекса программ и системы;
- оценка рисков с учетом регламентов и других требований поддержки применения комплексов программ;
- оценка альтернативных, конструктивных решений для сокращения рисков при проектировании комплекса программ.

На стадии производства и эксплуатации комплексов программ:

- контроль и оценка данных эксплуатации с целью сопоставления фактических показателей качества с соответствующими требованиями;

- обеспечение исходными данными процессов производства, методик эксплуатации, технического обслуживания, контроля и действий в чрезвычайных ситуациях проявления рисков;
- корректировка информации об основных источниках угроз, рисков и влияющих факторах;
- предоставление информации по значимости риска для принятия оперативных решений его сокращения;
- определение влияния на риски изменений в организационной структуре, производстве, процедурах эксплуатации и компонентах программного продукта и системы;
- подготовка персонала к применению программного продукта и системы при возможности проявления рисков.

Проявления рисков могут включать взаимосвязанные стоимостные и плановые виды рисков. ***Стоимостные риски*** составляют: нарушения ограничения суммарного бюджета проектирования и производства программного продукта; нарушения заданной ограниченной длительности производства компонентов и комплексов программ. ***Плановые риски*** включают: ущерб от дефектов стратегии и планирования проекта производства комплекса программ; достоверности планов, сроков и этапов жизненного цикла комплекса программ; нарушения требований и стандартов предотвращения, управления и сокращения рисков.

В проектах сложных систем, использующих программные продукты, риски могут быть обусловлены дефектами функциональных характеристик самих программ и их жизненного цикла, а также недостатками систем и внешней среды, в которой они используются. Основной ***ущерб от рисков программных продуктов*** проявляется в последствиях их применения – ***в дефектах и недостатках функционирования систем и внешней среды***. Поэтому анализ и оценка рисков комплексов программ должны быть тесно связаны с исследованием их проявления в системах, где они используются, причинами которых могут быть следующие ***виды рисков***: реализации функциональной пригодности программных продуктов; реализации конструктивных характеристик программного комплекса; ограничений ресурсов на проектирование и производство программного продукта. Результирующий ***ущерб*** в совокупности зависит от величины и вероятности проявления ***каждого вида риска***.

Риски реализации функциональной пригодности программных продуктов включают: **назначение; функции; масштаб – размер; сложность программного комплекса.**

Риски реализации конструктивных характеристик программного комплекса составляют: **корректность программ компонентов и комплекса; способность компонентов к взаимодействию; защищенность – безопасность; надежность – готовность; временная эффективность функционирования; сопровождаемость – изменяемость версий программного продукта.**

Риски ресурсов проектирования и производства программного продукта обусловлены ограничениями: **экономических и трудовых затрат; квалификации коллектива специалистов; технических, вычислительных ресурсов на проектирование, производство и функционирование программного продукта.**

При анализе и управлении сокращением рисков программных продуктов целесообразно выделять наиболее характерные этапы их ЖЦ: технико-экономического обоснование проекта; разработку требований спецификаций; проектирование; кодирование; тестирование; и документирование. При обосновании и реализации комплексов программ, анализ и управление их рисками должны являться частью общей ***проблемы обеспечения высокого качества проекта, предотвращения и сокращения рисков в системе и внешней среде*** [1, 2, 6]. Эти процессы состоят в выявлении возможных негативных отклонений характеристик комплекса программ и систем от требований контракта, технического задания и спецификаций, а также в создании базы для принятия мер по минимизации таких отклонений, с учетом ограниченных ресурсов на их реализацию и других факторов. Для этого при оценивании рисков программных продуктов, их необходимо трансформировать в величины возможных ***рисков для систем, среды и пользователей***, которые являются важнейшими и определяющими при применении программных продуктов. С точки зрения специалистов-разработчиков систем, принимающих решения, к основным ***методам анализа*** относятся:

- систематическая идентификация потенциальных опасностей, угроз и видов возможных отказов конкретной системы;
- количественные оценки или ранжирование опасности – ущерба от возможных рисков;
- оценка надежности и эффективности возможных контрмер и модификаций системы для снижения риска и достижения предпочтительных уровней ее качества;
- выявление факторов, обуславливающих возможный риск, и слабых звеньев в системе;
- сопоставление возможных рисков исследуемой системы с рисками альтернативных систем или технологий.

Ниже внимание сосредоточено ***на практических задачах и методологии*** анализа, оценивания и сокращения рисков программных продуктов, в процессе их проектирования и производства. Основные результаты обобщения моделей и факторов для сокращения рисков отражены ***этапами проектирования и производства***, которые рекомендуется выполнять при реализации базовых работ жизненного цикла сложных программных комплексов, и могут служить основой для разработки соответствующих планов работ при управлении, прогнозировании и сокращении рисков.

3. Подготовка исходных данных для анализа, прогнозирования и сокращения рисков комплексов программ

Обычно отсутствуют отдельные, предсказуемые факторы или методы, способные существенно изменять основные риски процесса разработки программ. Риски в ЖЦ комплекса программ могут быть обусловлены недостатками или непредумышленными, ***негативными действиями различных лиц***, участвующих в создании или применении системы и программного продукта. Основными ***источниками непредумышленных рисков*** программных продуктов, которые могут приводить к ущербу при их разработке и применении, являются:

- ***заказчики,*** определяющие назначение и функций системы и программного продукта, которые могут задавать некорректные или нереализуемые разработчиками требования к ним, а также ограничивают выделенные и доступные для проекта ресурсы: бюджет, время, затраты на технологию и инструментальные средства;
- ***разработчики*** системы и комплекса программ, обеспечивающие реализацию его ЖЦ, могут допускать дефекты и ошибки при обосновании проекта, не выполнять согласованные с заказчиком требования к характеристикам и качеству комплекса программ, а также превышать допустимое использование выделенных ресурсов, что может отражаться на проявлении и последствиях рисков на различных технологических этапах;
- ***менеджеры и эксперты управления рисками*** – координаторы взаимодействия заказчиков и разработчиков, которые уполномочены принимать решения о необходимости их изменения, путем применения необходимых контрмер, а также о допустимости применения системы и/или программного продукта с прогнозируемыми или достигнутыми, конкретными уровнями рисков.

Источниками и причинами рисков функционирования могут быть также ***пользователи***, некомпетентно применяющие систему или программный продукт с отклонениями от требований документации по функциональной пригодности или с недопустимым использованием ресурсов при эксплуатации.

Подготовка исходных данных для анализа и управления рисками программного продукта должна ***устанавливать источники*** подробной информацию о всех технических, связанных с окружающей средой, правовых, организационных и человеческих факторах, имеющих отношение к анализируемой проблеме, программному комплексу и системе, ***предположения*** о содержании, месте и условиях возможного проявления рисков. Следует сформулировать ожидаемые и возможные альтернативные решения, которые могут быть приняты, структура и описание предполагаемых рисков по результатам исследований

и от лиц, принимающих решения. Исходные данные проекта программного комплекса должны содержать:

- требования к функциям и характеристикам качества комплекса программ;
- описание и графическое представление его архитектуры, базы данных и взаимодействия компонентов;
- предполагаемую модель жизненного цикла комплекса программ;
- предварительные планы последующих этапов проектирования и производства комплекса программ;
- проекты технического задания и контракта на детальное проектирование и весь жизненный цикл комплекса программ [2, 6, 8].

Для этого следует подготовить ***требования к документации*** и обеспечить их реализацию, которая должна быть однозначной – написана в стандартизированных терминах, уточняемых, если необходимо, соответствующими комментариями. Должна быть выполнена первичная идентификация возможных опасностей, угроз и предварительная оценка возможных их последствий, являющихся причиной рисков. Известные потенциальные опасности должны быть четко и точно определены и описаны. Предварительную оценку значения идентифицированных опасностей – угроз необходимо выполнять, основываясь на анализе последствий рисков и изучении их основных причин у аналогичных проектов.

Программные продукты для обработки информации и управления обычно входят компонентами в системы более высокого уровня и зависят от внешней среды и функций системы, в которой они используются. Описания назначения, функций и требований к характеристикам системы, внешней среды и комплекса программ являются исходными данными трех взаимосвязанных технологических процессов:

- базовых, регламентированных ***технологических процессов и инструментария*** для их автоматизации, обеспечивающих проектирование и производство сложных программных продуктов;
- методов и средств обеспечения, требуемых характеристик комплекса программ на базе ***системы автоматизации контроля и обеспечения качества*** процессов и продуктов в их жизненном цикле;
- процессов и системы автоматизированного ***анализа, управления и сокращения рисков*** при создании и применении комплексов программ и систем в заданной внешней среде.

Для обеспечения высокого качества программного продукта целесообразно формировать группы экспертов для анализа угроз и управления рисками проектирования и производства программного продукта. Их следует ***выделять из основного жизненного цикла комплекса программ*** и поручать экспертам, разработку требований к функциональной пригодности и конструктивным характеристикам программного продукта с учетом возможных рисков[1, 2, 6].

4. Выделение, идентификация, анализ угроз и рисков в комплексах программ

В процессе управления проектом значительное внимание должно уделяться прогнозированию угроз и рисков, имеющих как внешние, так и внутренние причины. Этот ***этап анализа*** включает:

- выделение возможных источников и угроз нарушения требований и ограничений ресурсов в жизненном цикле комплекса программ, определение критериев функциональной работоспособности и/или отказа системы и программного продукта вследствие проявления рисков;
- идентификацию и анализ причин, выделение категорий и возможных последствий проявления рисков функциональной пригодности и конструктивных характеристик программного продукта;
- идентификацию и анализ причин, выделение категорий и возможных последствий рисков нарушения ограничений доступных ресурсов для проекта комплекса программ.

Накопленный опыт и обобщение проведенных исследований позволили выделить основные ***группы факторов*** [1, 5, 6], влияющих на риски при производстве комплексов программ:

- факторы, отражающие особенности создаваемого комплекса программ, как ***объекта*** разработки, требования к функциональным характеристикам и к качеству;
- факторы, определяющие ***организацию процесса*** разработки комплекса программ и его обеспечение квалифицированными специалистами;
- факторы, характеризующие ***технологическую среду*** и оснащенность инструментальными средствами автоматизации разработки комплекса программ;
- факторы, отражающие оснащенность производственного процесса ***аппаратурными вычислительными средствами***, на которых реализуются комплексы программ и базируются инструментальные системы автоматизации разработки.

Риски функциональной пригодности имеют доминирующее значение и изменения других видов рисков обычно должны быть, в первую очередь, подчинены сокращению этих рисков системы и комплекса программ. Цель и назначение программного продукта детализируются и формализуются в ***требованиях к функциям*** компонентов и всего комплекса программ, способного реализовать декларированные цели системы при отсутствии или допустимых рисках. Поэтому анализ рисков и возможных угроз целесообразно проводить систематизировано, начиная с рисков функциональной пригодности. Ущерб, вследствие ошибок функциональных требований к проекту программного комплекса может проявляться двумя видами рисков: недостатками достигнутых ***характеристик***, и рисками от нарушения ограничений доступных и используемых ***ресурсов*** в жизненном цикле комплекса программ. Предъявление заказчиком необоснованных требований к функциональной пригодности, проявления в них конфликтов и внутренних противоречий в содержании функций и компонентов, при реально доступных ресурсах и возможных условиях внешней среды применения, могут вызывать наиболее существенный ущерб в ЖЦ.

Цель и функции программного продукта реализуются тогда, когда ***выходная информация*** достигает потребителей – системы или операторов-пользователей, с требуемым содержанием и качеством, достаточным для обеспечения их эффективного применения. Степень покрытия всей выходной информацией: целей, назначения и функций для пользователей, следует рассматривать как ***основную меру рисков функциональной пригодности***. Прослеживание и оценивание адекватности и полноты состава выходной информации снизу вверх к назначению программного продукта должны завершать выбор базовых характеристик функциональной пригодности, независимо от сферы применения системы. При этом некоторые характеристики в реальном проекте могут приобретать значения более высокие, чем действительно требуются, на что нерационально расходуются ресурсы, а другие – не удовлетворять требованиям контракта и технического задания. Для разрешения этого противоречия основное значение имеет деятельность менеджера рисков, который должен ***прогнозировать***, проводить поэтапный анализ, контроль, оценивание и мониторинг возможных и реальных отклонений от требуемых характеристик и используемых ресурсов, ***управлять контрмерами и последовательно изменять их для сокращения интегрального риска*** всей системы.

Сокращение рисков конструктивных характеристик сложных комплексов программ целесообразно проводить с учетом их перечня в стандарте **ISO 9126**. Основной эффект по снижению рисков конструктивных характеристик может достигаться на начальных этапах проектирования, когда возможно предотвращение или сокращение многих из них с минимальными затратами времени и других ресурсов. Для этого в ***технологическом процессе производства*** необходимо использовать ***методы, которые включают***:

- систематизацию, документирование и оценивание эффективности доступных методов, средств и ресурсов контрмер для сокращения рисков функциональной пригодности и выделенных конструктивных характеристик;
- определение приоритетов конструктивных характеристик качества, компонентов и этапов ЖЦ, которые могут иметь потенциальные технические, стоимостные или плановые риски;
- оценивание вероятности каждого вида угроз конструктивной характеристики качества, потенциальной величины и вероятности их возможного негативного воздействия на каждую характеристику функциональной пригодности системы и программного продукта;

- оценивание уязвимости и возможных последствий дефектов каждой конструктивной характеристики и затрат ресурсов для восстановления требуемой функциональной пригодности при проявлении рисков;
- планирование и разработку решений по контрмерам для обеспечения допустимого уровня интегрального риска функциональной пригодности и конструктивных характеристик системы, в том числе возможно за счет изменения требований к программному продукту, системе и/или доступных ресурсов.

Риски ограничений доступных и используемых ресурсов в ЖЦ комплексов программ могут включать:

- экономические риски – превышение разработчиком обоснованных, допустимых по контракту размеров стоимости, трудоемкости и эксплуатационных затрат на программные компоненты и комплекс в целом, которые могут также отражаться на их функциональной пригодности и других характеристиках качества;
- плановые риски – нарушение разработчиком допустимых временных затрат в графиках работ, сроков реализации этапов и проекта в целом, а также распределений задач по подрядчикам, подразделениям и специалистам, что может также увеличивать риски характеристик;
- кадровые риски – недостаточная квалификация и число специалистов, отражающаяся на качестве разработки, совершенствования и/или применения программного продукта;
- технические риски – недостаточность вычислительных ресурсов, несогласованность ресурсов внутренней и внешней среды для реализации основных функций программного продукта;
- технологические риски – недостаточное качество инструментария для автоматизации всего ЖЦ и технологических процессов, предназначенных для обеспечения гарантированного сокращения рисков программного продукта;
- распределение ресурсов на контрмеры для сбалансированного сокращения интегрального риска комплекса программ и ответственности специалистов за реализацию сокращения рисков комплекса программ.

Прямые риски, обусловленные ошибками заданных экономических характеристик, могут вызвать ущерб заказчику при ***завышении стоимости проекта*** относительно реально необходимой, или ущерб разработчикам, если ***стоимость оценена недостаточной*** для его успешной реализации. Эти риски могут уменьшаться при последовательном уточнении размера комплекса программ на этапах формирования требований, предварительного и детального проектирования, однако они не полностью учитывают реальное влияние ограничений ресурсов на процессы и риски разработки и конечного программного продукта.

5. Сокращение и ликвидация опасных рисков, регистрация и утверждение допустимого интегрального риска программного продукта

Для выработки плана анализа рисков и применения контрмер их сокращения должна быть определена и документально установлена ***методика применения последовательного анализа угроз, уязвимостей и изменения проявления рисков*** [3, 7, 10]. После того как менеджеры проекта идентифицируют риски в жизненном цикле разработки, а также уточнят тактику итераций применения контрмер по сокращению их влияния, возникает необходимость в ***идентификации уровня допустимости остаточного риска***. В зависимости от требований к характеристикам, уровни допустимости рисков и контрмер могут варьироваться от качественных оценок до итерационных действий, предполагающих использование альтернативных подходов и дополнительных, последовательных разработок программных компонентов контрмер для сокращения рисков.

Совместное влияние на реализацию требований заказчика к комплексу программ, рисков характеристик программ и ресурсов для их реализации, должно быть ***сбалансировано контрмерами допустимого изменения*** тех и других видов рисков. В крайнем случае, если интегральный риск остается недопустимо большим, возможна по согласованию с заказчиком, ***корректировка требований к программному продукту или выделяемых ресурсов.*** Эти требования и ограничения могут не полностью выполняться на последующих этапах ЖЦ, что приводит к ущербу у заказчиков, разработчиков и пользователей. Причинами такого ущерба могут быть ошибки, а также завышенные заказчиком требования к характеристикам, которые не могут быть реализованы при выделенных ресурсах, или недостаточное качество технологии и квалификация специалистов – разработчиков, исполняющих проект. Если интегральные риски обусловлены недостаточной величиной одного из видов ресурса, то приходится перераспределять доступные ресурсы или искать заказчику способы увеличения некоторого, критического ресурса. В соответствие с их значениями следует откорректировать и утвердить обновленные, экономически и функционально оправданные, требования к характеристикам, используемым ресурсам и технологии. При любых стратегиях ***наиболее стабильными должны быть требования к функциональной пригодности комплекса программ***.

Для ***выбора критического уровня допустимых рисков*** необходимо исследовать особенности системы, последовательность возможного проявления потенциально опасных событий, любые смягчающие факторы и характеристики, а также природу и частоту возможных негативных последствий идентифицированных угроз в программном продукте и в системе. При этом для сбалансированного снижения интегрального риска, может оказаться эффективным сравнительное, количественное или качественное ранжирование рисков (при-

своение им приоритетов) специалистами, хорошо информированными ***в проблемной области*** применения соответствующих систем.

Используя ***планы управления рисками***, менеджер должен осуществлять распределение ресурсов контрмер, направленных на преодоление негативных случайностей. На начальных этапах жизненного цикла, инвестиции в проект постепенно растут вплоть до формулирования конкретных требований. Для обеспечения требуемого качества программных комплексов необходима ***организация контрмер*** в процессе управления рисками. Задача менеджера рисков состоит в выявлении и идентификации источников рисков, противоречий требований характеристик и ресурсов для их реализации и в предложении заказчику и разработчикам ***рациональных и возможных контрмер***, обеспечивающих сокращение рисков до допустимых пределов. Контрмеры для сокращения рисков можно разделить на три типа:

- сокращение или исключение ***первичных причин – угроз***, дефектов и ошибок в компонентах и комплексе программ, обусловленных недостатками их проектирования, разработки или модификации, отражающихся на рисках функциональной пригодности или характеристик комплексов программ;
- сокращение или ликвидация ***уязвимости*** компонентов программ и данных при воздействии на них угроз, дефектов и ошибок, путем введения средств защиты для блокирования их возможного негативного воздействия на риски функционирования и применения комплекса программ;
- непосредственное изменение и сокращение ***последствий проявления рисков*** функциональной пригодности, путем их оперативного обнаружения и ликвидации ущерба при сохранении (возможно) вызывающих их первичных источников и причин.

Крупные программные проекты постоянно усложняются, развиваются и модифицируются, вследствие чего весьма затруднительно рассматривать продукт как единое стабильное целое. В некоторых случаях процессы анализа и сокращения рисков могут быть упрощены [8]. Для этого целесообразно выделять и контролировать только отдельные (2 – 3), наибольшие по величине последствий и по вероятности проявления, риски отклонения от требований, и минимизировать возможный в результате ущерб для функциональной пригодности системы.

В процессах устранения рисков сложных комплексов программ, может участвовать большое число специалистов различных направлений и квалификации, которые, при необходимости, могут объединяться в ***службу сопровождения и управления конфигурацией программного продукта*** [4, 6, 10] (стандарт **ISO 15846**). Структура такой службы зависит от сложности и фазы развития проекта, от структуры предприятия, от ее взаимодействия с заказчиком и субподрядчиками и от ряда других факторов. Необходимо установить ***полномочия специалистов*** для выполнения контрмер и изменений рисков на каждом уровне проекта.

Основной задачей управления конфигурацией является документальное оформление и обеспечение полной наглядности выполняемых изменений, текущей конфигурации программ и данных и степени выполнения требований к их функциональной пригодности и конструктивным характеристикам при сокращении рисков. Другая задача заключается в том, чтобы все лица, работающие над проектом, в любой момент его жизненного цикла использовали достоверную и точную информацию о всех единицах конфигурации проекта и их взаимодействии. Изменения конфигурации комплекса и его компонентов при сокращении рисков должны планироваться и предусматривать действия с четкими разделами:

- ***почему*** и с какой целью производится корректировка программ или данных;
- ***кто*** персонально оценивает риски и выполняет контрмеры, санкционирует и утверждает проведение изменений комплекса или компонентов;
- ***какие*** действия и процедуры должны быть выполнены для реализации изменений рисков и конфигурации;
- ***когда*** по срокам и в координации, с какими другими процедурами ЖЦ следует реализовать определенную корректировку рисков и конфигурации комплекса программ;
- ***как*** и с использованием, каких методов, средств и ресурсов должны быть выполнены запланированные изменения комплекса программ и компонентов.

Для конкретного проекта должны быть определены и зафиксированы ***правила управление конфигурацией, документирования и утверждения интегрального риска версий***, применения административных и технологических процедур их мониторинга на всем протяжении жизненного цикла программного продукта. Организация документирования должна определять стратегию, стандарты, процедуры, распределение ресурсов и планы создания, изменения и применения документов на программы и данные. Для этого в общем случае должны быть выделены ***специалисты***, которые обязаны планировать, утверждать, выпускать, распространять и сопровождать комплекты утвержденных документов. Они должны стимулировать разработчиков программных средств, осуществлять непрерывное, регламентированное документирование процессов и результатов своей деятельности, а также контролировать полноту и качество утвержденного итогового отчета по результатам сокращения и ликвидации рисков программного продукта.

Литература

[1] Боэм Б.У. Инженерное проектирование программного обеспечения. Пер. с англ. /Под ред. А.А. Красилова. – М.: Радио и связь, 1985.

[2] Кантор М. Управление программными проектами. Практическое руководство по разработке успешного программного обеспечения. Пер. с англ. – М.: Вильямс. 2002.

[3] Липаев В.В. Анализ и сокращение рисков проектов сложных программных средств. – М.: СИНТЕГ. 2005.

[4] Липаев В.В. Отечественная программная инженерия: фрагменты истории и проблемы. – М.: СИНТЕГ. 2004.

[5] 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.

[6] Фатрелл Р. Т., Шафер Д. Ф., Шафер Л. И. Управление программными проектами: достижение оптимального качества при минимальных затратах. Пер. с англ. – М.: Вильямс. 2003.

[7] Boehm B.W. Software risk management. IEEE Computer Society Press. Washington. 1989.

[8] Charett R. Applications strategies for risk analysis. N.Y.: McGraw – Hill. 1989.

[9] Higuera R., Haimes Y. Software risk management. Pittsburg. Software engineering institute, Cornegie Mellon University. – 1996.

[10] Karolak D. W. Software engineering risk management. IEEE Computer Society Press. Washington. 1996.