П.29 Модели комплекса «Верификация»

П.29.1 Модель «Анализ степени влияния «подыгрывающих» компонентов и условий»

Анализ степени влияния «подыгрывающих» компонентов и условий функционирования системы осуществляется путем анализа возможностей системы к выполнению функций при замене еще не готовых компонентов на существующие аналоги в условиях, имитирующих штатный режим. Подобные замены при верификации используются для сокращения затрат и сроков создания системы, поскольку для сложных систем натурные испытания в большом объеме очень дорогостоящи и в силу многовариантности реальных условий эксплуатации все равно не позволяют в полной мере оценить реальные возможности системы. Для моделирования необходима информация о характеристиках архитектурных решений, подлежащих проверке с использованием «подыгрывающих» компонентов и условий, функциональных возможностях каждого из компонентов и оперативного восстановления временно утрачиваемых функциональных возможностей системы с учетом штатных мер поддержания работоспособности и при верификации, а также о требованиях к сроку сохранения приемлемого качества функционирования системы.

Модель развивает положения модели П.23.3 «Определение характеристик среды функционирования» комплекса «ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ ЗАКАЗЧИКА» в части сравнения возможностей системы для различных вариантов состава и сопровождения ресурсов. В качестве исходных данных используются:

для характеристики архитектурных решений, подлежащих проверке с использованием «подыгрывающих» компонентов и условий

взаимосвязь подсистем и составных компонентов; номер подсистемы (n) в моделируемой структуре;номер составного компонента в n–й подсистеме (k);

для характеристики возможностей k-го компонента с учетом штатных мер поддержания работоспособности и при верификации

наработка по требованиям заказчика; наработка при верификации;

для характеристики оперативного восстановления временно утрачиваемых функциональных возможностей системы

время восстановления по требованиям (среднее); время восстановления при верификации (среднее);

для характеристики требований к сроку сохранения приемлемого качества

задаваемый срок службы системы; длительность процесса верификации.

В результате расчетов оцениваются:

наработка на нарушение приемлемого качества функционирования n–й подсистемы в штатном режиме ($T_{нар.\,n}$);

наработка на нарушение приемлемого качества функционирования n–й подсистемы при верификации ($T_{нар.вериф.\,n}$);

наработка на нарушение приемлемого качества функционирования системы в штатном составе и условиях ($T_{нар.}$);

наработка на нарушение приемлемого качества функционирования системы при верификации ($T_{нар.вериф.}$);

вероятность качественного функционирования системы в штатном составе и условиях в течение срока службы (P);

вероятность качественного функционирования системы при использовании «подыгрывающих» компонентов и условий в течение срока верификации ($P_{вериф.}$);

вероятность качественного функционирования системы в штатном составе и условиях в течение срока верификации ($P_{сравн.}$);

вероятность качественного функционирования системы при использовании «подыгрывающих» компонентов и условий в течение срока службы ($P_{вериф.сравн.}$);

Расчеты осуществляются на основе использования модели П.23.3 «Определение характеристик среды функционирования» для требований заказчика и условий верификации. Используемые для моделирования функциональная структура и состав ресурсов, их взаимосвязи (полная независимость, последовательная зависимость, дублирование функций, холодный или горячий резерв), режимы использования и сопровождения определяются вариантами ресурсного обеспечения при эксплуатации и верификации системы или в сравнении с аналогами. Наработка каждого из компонентов на нарушение приемлемого качества и время восстановления работоспособности системы определяются материальными запасами и стратегией технического обслуживания, надежностью и безопасностью технических и программных средств, качеством используемой информации, подготовленностью персонала, что может быть получено с использованием натурных экспериментов, моделирования или сравнением с аналогами. Срок службы системы продукции задается в контрактных условиях заказчика, длительность процедуры верификации определяется технической политикой руководства предприятия и заказчика.

П.29.2 Модель «Анализ степени соответствия»

Анализ степени соответствия проводится для отдельных составных компонентов и для системы в целом. Предлагаемые ниже модели позволяют осуществлять как автономное моделирование объектов (компонентов, подсистем, систем), выполняющих функции систем массового обслуживания, сбора, контроля, анализа, мониторинга, противодействия угрозам, так и комплексное функционирование объектов. Степень соответствия осуществляется путем сравнения интегральных показателей функционирования объектов с задаваемыми требованиями заказчика.

П.29.2-1 «Верификация объекта, выполняющего функции системы массового обслуживания»

Модель позволяет оценить интегральные вероятностно-временные характеристики объекта, выполняющего функции системы массового обслуживания различного рода запросов Моделирование осуществляется в соответствии с положениями, изложенными в модели П.23.4 «Определение характеристик взаимодействия пользователей с системой» комплекса «ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ ЗАКАЗЧИКА».

В результате расчетов оцениваются: среднее время обработки запросов i-го типа (T_i), вероятность своевременной обработки запросов i –го типа за заданное время (P_i), относительная доля своевременно обработанных запросов всех типов (S), относительная доля своевременно обработанных запросов лишь тех типов, для которых выполняются требования заказчика (C).

Расчеты осуществляются с использованием модели П.2 «Комплекс моделей процессов обработки запросов в системе».

Используемые для моделирования интенсивность запросов и среднее время обработки запросов определяются требованиями ТЗ, результатами натурных экспериментов, дополнительным моделированием или в сравнении с аналогами. Технология обработки

запросов либо конструируется (в том числе по результатам моделирования для оптимизации процессов), либо берется за основу сложившийся способ регулирования очередей при доступе и расходовании ресурсов. Временные ограничения на удовлетворение потребностей в ресурсах определяются критерием своевременности, принятым в системе для каждого из типов запросов с точки зрения оптимизации процессов функционирования.

П.29.2-2 «Верификация объекта, выполняющего функции системы сбора»

Моделирование объекта, выполняющего функции системы сбора, обеспечивается на основе анализа данных о возможных характеристиках системы сбора чего-либо (далее по тексту «собираемых объектов» – информации, составных элементов и др.) от источников. Сбор включает в себя обновление собираемых объектов, утрачивающих со временем свои потребительские свойства, а также об изменениях, значимых для достижения целей сбора и характеризующих пригодность собираемых объектов для последующего целевого использования. Модель основана на применении модифицированной модели П.4 «Комплекс моделей процессов сбора объектов от источников (информации, составных элементов и др.)» с точностью до смыслового переопределения исходных данных.

В качестве исходных данных используются:

для характеристики изменений, значимых для достижения целей сбора и характеризующих пригодность собираемых объектов для использования

частота значимых изменений;

для характеристики системы сбора объектов от источников (в т.ч. обновления собираемых объектов, утрачивающих со временем свои потребительские свойства)

время подготовки объекта у источников (среднее); время доведения до получателя (среднее); время приема у получателя (среднее);

дисциплина сбора объектов от источников (D), где $D = D_1$ означает что объекты собираются «сразу по происшествии значимого изменения», $D=D_2$ означает, что объекты собираются вне явной зависимости от происшествия изменений; частота сбора объектов для дисциплины D_2**.**

В результате расчетов оценивается вероятность сохранения потребительских свойств собираемых объектов на момент их использования (P), причем только для дисциплины D_2 вводится дифференциация: $P_{строг.}$ означает расчетную вероятность P для случая, когда время между моментами очередного сбора объектов строго постоянно, а $P_{нестрог.}$ – когда время между моментами очередного сбора объектов непостоянно (распределено экспоненциально). Расчеты осуществляются с применением модели П.4 «Комплекс моделей процессов сбора информации от источников».

Используемая для моделирования частота значимых изменений устанавливается в результате дополнительного моделирования, натурных экспериментов или сравнения с аналогами с учетом утрачивания со временем потребительских свойств объектов. Возможные значения времен подготовки объекта у источников, доведения до получателя и приема у получателя, а также дисциплины сбора объектов определяются руководством в соответствии с функциями системы, критериями целесообразности и проводимой технической политикой.

П.29.2-3 «Верификация объекта, выполняющего функции системы контроля»

Требуемое качество проверки каких-либо контролируемых объектов обеспечивается на основе использования эффективных средств и способов выявления брака (ошибок, дефектов, несоответствий и пр.) и рациональной регламентации работы контролера. Моделирование компонента основано на модифицированном применении модели П.5 «Модель процессов анализа объектов (информации, образцов, событий и др.)» с точностью до смыслового переопределения исходных данных. В качестве исходных данных используются:

для характеристики контролируемых объектов

количество контролируемых объектов; доля первоначального брака до контроля %;

для характеристики технологии контроля

скорость контроля; частота ошибок контроля 1-го рода, когда объект приемлемого качества квалифицируется как брак; наработка контролера на ошибку 2-го рода, т.е. до момента, когда брак оказывается пропущенным; период непрерывной работы контролера;

для характеристики временных ограничений

допустимое время контроля.

В результате расчетов оценивается риск наличия брака в проверенном объеме (R), определяемый как обратная величина вероятности отсутствия брака (ошибок) в проверенном объеме за отведенное время.

Используемые для моделирования пределы исходных значений количества контролируемых объектов и допустимого времени контроля задаются в ТЗ на разработку системы, в эксплуатационной документации или инструкциях должностным лицам. Возможные значения доли первоначального брака до контроля, скорости контроля, частоты ошибок контроля 1-го рода и наработки контролера на ошибку 2-го рода устанавливаются в результате натурных экспериментов, дополнительного моделирования или сравнения с аналогами. Значение периода непрерывной работы контролера указывается в эксплуатационной документации как характеристика регламента труда и отдыха в течение рабочего дня.

П.29.2-4 «Верификация объекта, выполняющего функции системы анализа»

Моделирование объекта обеспечивается на основе учета следующих положений. Корректность анализа каких-либо объектов (информации, образцов, событий и др.) обеспечивается на основе использования эффективных для этих целей способов, которые позволяют учесть существенные анализируемые объекты и не допустить ошибок в реальных условиях функционирования системы. Корректность является следствием приемлемого соотношения между количеством объектов, подлежащих анализу, долей существенных объектов для целей анализа, скорости анализа, частоты допускаемых ошибок, периода непрерывной работы аналитика (автоматизированного средства или человека в совокупности с используемыми им средствами анализа) и ограничений на допустимое время анализа.

Модель основана на модифицированном применении модели П.5 «Модель процессов анализа объектов (информации, образцов, событий и др.)» с точностью до объединения в одну переменную частоту ошибок 1-го и 2-го рода и смыслового переопределения исходных данных. В качестве исходных данных используются:

для характеристики анализируемых объектов

количество объектов, подлежащих анализу; доля существенных объектов для целей анализа %;

для характеристики технологии анализа

скорость анализа; частота ошибок; период непрерывной работы при анализе, для человека определяется регламентом труда и отдыха в течение рабочего дня;

для характеристики временных ограничений

допустимое время на анализ.

В результате расчетов оценивается вероятность получения корректных результатов анализа (P) за отведенное время.

Используемые для моделирования пределы исходных значений количества объектов, подлежащих анализу и допустимого времени на анализ задаются в ТЗ на разработку системы, в эксплуатационной документации или инструкциях должностным лицам. Возможные значения доли существенных объектов для целей анализа, скорости анализа и частоты ошибок устанавливаются в

результате натурных экспериментов, дополнительного моделирования или сравнения с аналогами. Значение периода непрерывной работы аналитика-человека указывается в эксплуатационной документации как характеристика регламента труда и отдыха в течение рабочего дня. Если в качестве аналитика используются автоматизированные средства, период непрерывной работы может совпадать с наработкой этих средств на отказ.

П.29.2-5 «Верификация объекта, выполняющего функции системы мониторинга»

Моделирование объекта обеспечивается на основе учета следующих положений. Реакция оператора на критичные отклонения в системе полагается своевременной в течение заданного периода ее функционирования, если к началу оцениваемого периода мониторинга целостность системы обеспечена и в течение всего периода либо критичные отклонения не возникают, либо не происходит развития критичной ситуации до угрожающих пределов.

Моделируемая технология выявления критичных отклонений основана на периодических контролях целостности системы и мониторинге критичных процессов и объектов между моментами системного контроля. Результатом применения очередного контроля целостности является полное восстановление нарушенной целостности системы или подтверждение целостности при отсутствии ее нарушения. Выявление нарушений целостности возможно лишь в результате контроля или безошибочной работы оператора (автоматизированного средства или человека в совокупности с используемыми средствами мониторинга) между моментами контроля. Целостность системы может оказаться нарушенной лишь после развития критичной ситуации до угрожающих пределов, если в результате допущенной ошибки таковое опасное развитие не было своевременно выявлено оператором. До превращения критичной ситуации в реальную угрозу штатный режим функционирования системы считается соблюденным.

Достижение своевременной реакции на критичные отклонения при мониторинге является следствием достаточно частого контроля целостности системы и безошибочной работы оператора в процессе мониторинга.

Модель основана на модифицированном применении модели П.6 «Комплекс моделей опасных воздействий на защищаемую систему» (см. технологию 3) с точностью до смыслового переопределения исходных данных в приложении к оператору, реализующему функции мониторинга. В качестве исходных данных используются:

для характеристики угроз

частота появления критичных отклонений (например, для качества или безопасности системы);

среднее время развития критичной ситуации до угрожающих пределов;

для характеристики системы мониторинга

время между моментами контроля целостности (окончанием предыдущего и началом очередного); длительность контроля целостности; наработка оператора на ошибку (при мониторинге между соседними моментами контроля целостности);

для характеристики периода функционирования системы (для оценки)

задаваемый период функционирования.

В результате расчетов оценивается вероятность своевременной реакции на критичные отклонения (P) и риск пропуска критичных отклонений в режиме реального времени (R) как обратная величина от вероятности P.

Используемые для моделирования пределы исходных значений задаваемого периода функционирования, частоты появления критичных отклонений и среднего времени развития критичной ситуации до угрожающих пределов задаются в ТЗ на разработку системы, в эксплуатационной документации или инструкциях должностным лицам при указании сценариев возможного опасного воздействия на систему. Значение наработки оператора на ошибку и длительность контроля целостности устанавливается в результате натурных экспериментов в зависимости от применяемых технологий, программно-технических средств и способов мониторинга. Значение времени между моментами контроля целостности указывается в эксплуатационной документации.

П.29.2-6 «Верификация объекта, выполняющего функции системы противодействия угрозам»

Проектирование объекта как системы противодействия угрозам должно быть направлено на минимизацию риска негативного воздействия на систему в течение различных периодов потенциальной опасности. Модель развивает положения модели П.7 «Комплекс моделей процессов несанкционированного доступа к ресурсам системы» с точностью до переопределения исходных данных и выходных результатов в предположении независимости мер противодействия угрозам. В качестве исходных данных используются:

для характеристики m–й меры противодействия угрозам

время сохранения эффективности меры с момента начала ее применения до утраты приемлемой способности противодействия угрозам (прогнозируемое);

время до очередного адекватного усиления меры, приводящего к восстановлению ее приемлемой эффективности;

для характеристики периода функционирования системы при оценке

длительность периода потенциальной опасности (ожидаемая).

В результате расчетов оценивается риск опасного воздействия на систему вопреки мерам противодействия (R).

Расчеты осуществляются с использованием модели П.7 «Комплекс моделей процессов несанкционированного доступа к ресурсам системы».

Используемое для моделирования время сохранения эффективности меры противодействия угрозам определяется результатами натурных экспериментов, дополнительного моделирования, реальных проверок или в сравнении с аналогами. Время до очередного адекватного усиления меры, приводящего к восстановлению ее приемлемой эффективности, регламентируется руководством и службой безопасности с учетом важности и сложности работ и проводимой технической политики.

П.29.2-7 «Верификация комплексного функционирования системы»

Верификация комплексного функционирования системы замыкается на оценку ее интегрального качества, т.е. способности выполнять функции с приемлемым качеством в течение всего срока службы. Моделирование обеспечивается на основе анализа данных об архитектурном построении системы, оперативном восстановлении временно утрачиваемых функциональных возможностей, о характеристиках автономных возможностей каждого из объектов (без использования мер поддержания его работоспособности) и системных мер обеспечения приемлемого качества компонента, требований к максимально допустимому риску нарушения приемлемого качества компонента, а также требований к сроку непрерывного сохранения приемлемого качества функционирования системы. Модель базируется на использовании модели П.25.1 Модель «Анализ проекта архитектурного построения системы» комплекса «ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ».

В качестве исходных данных используются:

для характеристики варианта архитектурного построения системы

взаимосвязь подсистем и составных компонентов; номер подсистемы (n) в моделируемой структуре;номер составного компонента в n–й подсистеме (k);

для характеристики оперативного восстановления временно утрачиваемых функциональных возможностей системы

время восстановления (среднее);

для характеристики требований к сроку непрерывного сохранения приемлемого качества функционирования

срок службы системы;

для характеристики требований заказчика к минимально допустимой вероятности обеспечения приемлемого качества функционирования системы

допустимая вероятность;

для характеристики требования к максимально допустимому риску нарушения приемлемого качества k-го компонента в системе

максимальный риск;

для характеристики автономных возможностей k-го компонента без использования мер поддержания его работоспособности в системе

наработка на нарушение работоспособности;

для характеристики системных мер обеспечения приемлемого качества k-го компонента в системе

период между моментами восстановления требуемой функциональной работоспособности;

затраты на обеспечение функционирования в единицу времени.

В результате расчетов оцениваются: наработка на нарушение приемлемого качества функционирования n–й подсистемы ($T_{нар\ n}$), наработка на нарушение приемлемого качества функционирования системы ($T_{нар}$), вероятность обеспечения приемлемого качества функционирования системы (P), затраты на обеспечения функционирования системы в единицу времени и за весь срок службы.

Расчеты осуществляются с использованием моделей П.23.1 «Определение требований к интегральному качеству» и П.23.3 «Определение характеристик среды функционирования».

Используемые для моделирования наработка на нарушение работоспособности компонента (т.е. до момента нарушения штатного режима функционирования системы) и время восстановления определяются результатами натурных экспериментов, дополнительного моделирования, реальных проверок или в сравнении с аналогами. Функциональная структура ресурсов, их взаимосвязи (полная независимость, последовательная зависимость, дублирование функций, холодный или горячий резерв) и затраты на обеспечение функционирования в единицу времени определяются вариантами ресурсного обеспечения системы или в сравнении с аналогами. Максимально допустимый риск нарушения приемлемого качества каждого из компонентов определяется разработчиком исходя из требований заказчика к интегральному качеству системы, ее важности, сложности и осуществляемых системных мер обеспечения работоспособности с учетом затрат. Период между моментами штатного восстановления требуемой функциональной работоспособности компонента регламентируется руководством и службой качества с учетом важности и сложности системы и проводимой технической политики.

П.29.3 Модель «Анализ качества верификации»

Анализ качества верификации осуществляется с использованием данных о характеристиках полного объема объектов и процессов, которые влияют на выполнение требований заказчика, характеристиках объектов и процессов, проверяемых при верификации, функциональных возможностей проверяющих специалистов и привлекаемых средств для верификации, а также временных ограничений на длительность верификации.

Модель основана на модифицированном использовании модели П.5 «Модель процессов анализа объектов (информации, образцов, событий и др.)» с точностью до смыслового переопределения исходных данных.

В качестве исходных данных используются:

для характеристики полного объема объектов и процессов, которые влияют на выполнение требований заказчика

количество объектов и процессов; доля реальных несоответствий;

для характеристики объектов и процессов, проверяемых при верификации

количество объектов и процессов;

для характеристики функциональных возможностей проверяющих специалистов и привлекаемых средств верификации

скорость проверки; частота пропуска реального несоответствия; продолжительность непрерывной проверки;

для характеристики временных ограничений на длительность верификации

длительность.

В результате расчетов оцениваются: вероятность выявления несоответствий при верификации (P_j) и

доля невыявленных несоответствий при верификации (F_j).

Расчеты проводятся с использованием модели П.5 «Модель процессов анализа объектов (информации, образцов, событий и др.)».

Используемые для моделирования количество проверяемых при верификации и полное множество объектов и процессов, а также длительность верификации определяются контрактами и руководством в зависимости от сложности создаваемой системы и в соответствии с проводимой на предприятии технической политикой при выполнении проекта. Скорость проверки, доля реальных несоответствий, частота пропуска реального несоответствия определяется результатами реальных проверок, с помощью дополнительного моделирования или в сравнении с аналогами. Продолжительность непрерывной проверки является характеристикой регламента труда и отдыха при выполнении верификационных работ.

П.29.4 Модель «Анализ стратегии верификации»

Анализ стратегии верификации осуществляется с использованием данных о характеристиках полного объема объектов и процессов, которые влияют на выполнение требований заказчика, характеристиках объектов и процессов, проверяемых при верификации, функциональных возможностей проверяющих специалистов и привлекаемых средств для верификации, а также временных ограничений на длительность верификации.

Модель основана на развитии модели П.29.3 Модель «Анализ качества верификации» в части учета полного множества различных проверяемых требований проекта.

Для каждого из типов проверяемых требований в качестве исходных данных используются:

для характеристики полного объема объектов и процессов, которые влияют на выполнение требований заказчика

количество объектов и процессов (V_i); доля реальных несоответствий;

для характеристики объектов и процессов, проверяемых при верификации согласно принятой стратегии

количество объектов и процессов;

для характеристики функциональных возможностей проверяющих специалистов и привлекаемых средств верификации

скорость проверки; частота пропуска реального несоответствия; продолжительность непрерывной проверки;

для характеристики временных ограничений на длительность верификации

длительность.

В результате расчетов оцениваются: вероятность выявления несоответствий требованиям i –го типа (P_i),

доля невыявленных несоответствий требованиям i –го типа (F_i), вероятность успешного воплощения стратегии верификации (P), доля невыявленных несоответствий после верификации (F).

Расчеты вероятности выявления несоответствий требованиям i –го типа (P_i) и доли невыявленных несоответствий требованиям i –го типа (F_i) проводятся с использованием модели П.29.3 Модель «Анализ качества верификации». Вероятность успешного воплощения стратегии верификации (P) по сути представляет собой вероятность выявления всех несоответствий за время верификации. В предположении независимости типов проверяемых требований она рассчитывается по формуле:

$$P = \prod_{i=1}^{I} P_i$$

Доля невыявленных несоответствий после верификации (F) рассчитывается по формуле: $F = \sum_{i=1}^{I} F_i V_i \Big/ \sum_{i=1}^{I} V_i$.

Используемые для моделирования количество проверяемых при верификации и полное множество объектов и процессов, а также длительность верификации определяются контрактами и руководством в зависимости от сложности создаваемой системы и в соответствии с проводимой на предприятии технической политикой при выполнении проекта. Скорость проверки, доля реальных несоответствий, частота пропуска реального несоответствия определяется результатами реальных проверок, с помощью дополнительного моделирования или в сравнении с аналогами. Продолжительность непрерывной проверки является характеристикой регламента труда и отдыха при выполнении верификационных работ.