Аналитическая записка

В.В. Гантимуров

Аннотация

Данный документ разработан с целью минимизации трудозатрат аналитиков при разработке Технических заданий на автоматизированные системы на основе порталов. Для этого, кроме примеров требований (в приложениях), приводятся рекомендации по выбору состава требований, показателей надежности и их наполнению (содержанием и смыслом). Изложенные рекомендации при необходимости могут служить примером обоснования требований по надежности. Данные рекомендации не исключают необходимости изучения указанных стандартов, а всего лишь призваны облегчить ориентацию в них.

Предполагается, что изложенные в приложениях примеры разделов ТЗ по надежности будут взяты за основу и доработаны с учетом специфики и конкретики разрабатываемых систем.

Изложенные рекомендации и примеры требований по надежности ни в коей мере не являются исчерпывающими. Это всего лишь основа, которая, возможно, позволит быстро в первом приближении и с пониманием сути вопроса заполнить соответствующие разделы ТЗ.

Часть пояснений, особенно в приложениях, для привязки к тексту изложена в примечаниях, поэтому рекомендуется использовать режим отображения примечаний в редакторе MS Word.

При работе над документом были учтены замечания и предложения сотрудников Отделения системного анализа Сурена Манасова, Анастасии Карпухиной, Криковцевой Инны, в чем им искренняя благодарность за потраченные усилия и время.

Содержание

1. Общие положения

ГОСТ 27.003-90[1] трактует требования по надежности как совокупность количественных и (или) качественных требований к безотказности, долговечности, ремонтопригодности, сохраняемости, выполнение которых обеспечивает эксплуатацию изделий с заданными показателями эффективности, безопасности, экологичности, живучести и других составляющих качества, зависящими от надежности изделия, или возможность применения данного изделия в качестве составной части другого изделия с заданным уровнем надежности.

Этим определением охвачены свойства изделия, которые составляют и само понятие и, по сути, указывают на комплексный характер свойства надежности. В качестве таких свойств указаны:

1. безотказность,
2. долговечность,
3. ремонтопригодность.
4. сохраняемость.

Исходя из определения, уже можно говорить о структуре требований по надежности, по крайней мере, для изделия.

Более того, ГОСТ 27.003 указывает конкретно, какие требований по надежности (для изделий) должны быть заданы:

1. типовая модель эксплуатации (или несколько моделей), применительно к которой (которым) задают требования по надежности;
2. критерии отказов по каждой модели эксплуатации, применительно к которой задают требования по безотказности;
3. критерии предельных состояний изделий, применительно к которым установлены требования по долговечности и сохраняемости;
4. понятие "выходной эффект" для изделий, требования по надежности к которым установлены с использованием показателя "коэффициент сохранения эффективности" $K_{эф}$;
5. номенклатуру и значения показателей надежности (ПН), применительно к каждой модели эксплуатации;

[1] Надежность в технике. Состав и общие правила задания требований по надежности

6. методы контроля соответствия изделий заданным требованиям по надежности (контроля надежности);
7. требования и (или) ограничения по конструктивным, технологическим и эксплуатационным способам обеспечения надежности, при необходимости, с учетом экономических ограничений;
8. необходимость разработки программы обеспечения надежности (ПОН).

Структура требований к автоматизированным системам (АС) по надежности определена в ГОСТ 34.602-89[2]. В требования по надежности включают:

1) состав и количественные значения показателей надежности для системы в целом или ее подсистем;

2) перечень аварийных ситуаций, по которым должны быть регламентированы требования по надежности, и значения соответствующих показателей;

3) требования по надежности технических средств и программного обеспечения;

4) требования к методам оценки и контроля показателей надежности на разных стадиях создания системы в соответствии с действующими нормативно-техническими документами.

При разработке автоматизированных систем управления (АСУ) всех видов и уровней управления, кроме общегосударственного – обязательном порядке, а также при разработке требований по надежности для автоматизированных систем в части порядка установления требований, оценки показателей надежности, состава и порядка проведения работ по обеспечению надежности рекомендуется учитывать ГОСТ 24.701-86[3]. Данный стандарт не устанавливает состав требований по надежности (не следует путать с составом показателей надежности), в нем изложены основные положения о порядке и правилах разработки указанных требований.

Кроме того, при разработке отдельных требований, касающихся средств вычислительной техники, может быть полезен ГОСТ 21552-84[4]. Данный стандарт распространяется на стационарные средства вычислительной техники (СВТ), применяемые в автоматизированных системах управления различного назначения всех уровней, в системах обработки данных, сетях ЭВМ, на вычислительных центрах автономно, а также встраиваемые в машины, оборудование и приборы, и предназначенные для сбора, подготовки, ввода, накопления, обработки, вывода, отображения, приема и передачи информации, и устанавливает требования к СВТ, изготовляемым для народного хозяйства и экспорта.

2. Состав и количественные значения показателей надежности для системы в целом или ее подсистем

Анализ состава требований по надежности, изложенных в указанных ГОСТах, позволяет сделать вывод, что структура требований по ГОСТ 34 является более

[2] Полное название стандарта «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

[3] Полное название "Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения".

[4] Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение.

общей. Раскрытие каждого из пунктов требований по надежности по ГОСТ 34 целесообразно выполнять, руководствуясь требованиями ГОСТ 27.

Так, например, раскрывая пункт требований «Состав и количественные значения показателей надежности для системы в целом или ее подсистем» необходимо руководствоваться следующими положениями ГОСТ 27.003-90:

1. Пунктами 1.4 – 1.8: общие требования к показателям надежности;
2. Раздел 3 «Выбор номенклатуры задаваемых показателей надежности»;
3. Раздел 4 «Выбор и обоснование значений показателей надежности»;
4. Приложением 2 «Примеры возможных модификаций и определений стандартизованных показателей»;
5. Приложением 3 «Методика выбора номенклатуры задаваемых показателей надежности».

Более того, целесообразно изложить в начале этого пункта ТЗ или в отдельном пункте, но выше, требования, которым должна удовлетворять система в части модели эксплуатации.

Например:

Система должна относиться к обслуживаемым восстанавливаемым изделиям общего назначения непрерывного длительного применения согласно ГОСТ 27.003-90. Основные показатели надежности Системы согласно ГОСТ 24.701-86 и ГОСТ 27.003-90:

- *коэффициент готовности системы $К_г$;*
- *среднее время восстановления работоспособности $Т_в$.*

На модель эксплуатации указывают следующие перечисленные признаки:

- *система обслуживаемая,*
- *система восстанавливаемая,*
- *система общего назначения непрерывного длительного применения.*

Это типичный набор признаков системы, которому ГОСТ 27.003 ставит в соответствие указанные показатели надежности.

В общем случае для выбора показателей надежности необходимо уметь пользоваться следующей таблицей (из ГОСТ 27.003). Для этого следует правильно позиционировать (классифицировать) разрабатываемую систему.

Таблица 1- Обобщенная схема выбора номенклатуры задаваемых ПН

Характеристика изделия			Номенклатура задаваемых ПН
ИКН[5]	Вид II[6]	Восстанавливаемое и невосстанавливаемое	Коэффициент сохранения эффективности $K_{эф}$ или его модификации (примеры возможных модификаций $K_{эф}$ приведены в приложении 2 ГОСТ 27.003-90); показатели долговечности, если для изделия может быть однозначно сформулировано понятие "предельное состояние" и определены критерии его достижения; показатели сохраняемости, если для изделия предусматривается хранение (транспортирование) в полном составе и собранном виде или показатели сохраняемости отдельно хранимых (транспортируемых) частей изделия

[5] ИКН - изделия конкретного назначения, имеющие один основной вариант применения по назначению. Для систем характерно более одного варианта применения.

[6] Изделия вида II, которые, кроме указанных двух состояний, могут находиться в некотором числе частично неработоспособных состояний, в которые они переходят в результате частичного отказа.

	Вид I[7]	Восстанавливаемое	Комплексный ПН и, при необходимости, один из определяющих его показателей безотказности или ремонтопригодности (в соответствии с п. 1.7 ГОСТ 27.003-90); показатели долговечности и сохраняемости, выбираемые аналогично изделиям вида II
		Невосстанавливаемое	Единичный показатель безотказности; показатели долговечности и сохраняемости, выбираемые аналогично изделиям вида II
ИОН[8]	Вид II	Восстанавливаемое и невосстанавливаемое	Набор ПН составных частей изделия, рассматриваемых как изделия вида I
	Вид I	Восстанавливаемое	Комплексный ПН и, при необходимости, один из определяющих его показателей безотказности или ремонтопригодности (в соответствии с п. 1.7 ГОСТ 27.003-90); показатели долговечности и сохраняемости, выбираемые аналогично ИКН вида I
		Невосстанавливаемое	Единичный показатель безотказности; показатели долговечности и сохраняемости, выбираемые аналогично ИКН вида I

Кроме указанных в таблице признаках изделия различают по режимам применения (функционирования) на следующие:

1. изделия непрерывного длительного применения;
2. изделия многократного циклического применения;
3. изделия однократного применения (с предшествующим периодом ожидания применения и хранения)

Как правило, для АС (особенно информационных на основе порталов[9]) характерно несколько вариантов применения и при этом они являются восстанавливаемыми. Если в системе предусмотрено резервирование программно-аппаратных средств, или резервное копирование, то это в явном виде указывает на то, что система имеет более одного варианта применения. Кроме того, число состояний[10] для сложных систем, состоящих из большого числа подсистем, аппаратных и программных средств, и других компонент, может быть довольно значительным. Строго говоря, поэтому АС следует относить к восстанавливаемым ИОН вида II. Однако при отсутствии возражений со стороны Заказчика и при наличии критериев отказа[11] или неработоспособного состояния АС можно отнести к восстанавливаемым ИОН вида I.

С точки зрения режимов применения АС можно отнести к изделиям непрерывного длительного применения или многократного циклического применения. Последний вариант возможен при задании требований, например по обязательному техническому обслуживанию, или ожиданию применения, или хранения, с определением временных циклов (границ) указанных этапов эксплуатации.

В соответствии с указанной таблицей и с учетом выбора режима непрерывного длительного применения возможно использование комплексного показателя надежности, например коэффициента готовности системы (подсистемы) в целом или для составляющих ее программно-технических комплексов отдельности.

Под коэффициентом готовности понимают вероятность того, что система в произвольный момент времени будет готова к применению. Коэффициент готовности $K_г$ системы считается комплексным показателем, поскольку его значение определяется множеством различных факторов случайного характера, что и находит

---

[7] Изделия вида I, которые в процессе эксплуатация могут находиться в двух состояниях - работоспособном или неработоспособном;

[8] Изделия общего назначения (ИОН), имеющие несколько вариантов применения

[9] Здесь и далее рассматриваются автоматизированные информационные системы на основе порталов.

[10] Число состояний системы определяется числом состояний по каждой из компонент.

[11] Формулировка критерия (критериев) отказа должна четка определять признаки неработоспособного состояния системы в целом.

свое отражение в определении:

,

где T_o – среднее время наработки на отказ.

В требованиях дополнительно к указанию значений коэффициента готовности, как правило, излагают требования и ко времени восстановления системы в единицах времени.

При задании в модели эксплуатации в явном виде сроков проведения ТО различных видов[12] возможно указание коэффициента оперативной готовности системы. Но такого рода нюансы определяются системой эксплуатации и нормативными документами Заказчика, что в настоящем документе не рассматривается.

3. Перечень аварийных ситуаций

Перечень аварийных ситуаций в общем случае зависит от назначения системы, ее состава и режимов функционирования, в пределах которых необходимо обеспечить заданные характеристики функционирования. Во многом назначение и режимы функционирования определяют типовую модель эксплуатации (или несколько моделей), требования к которой определены в ГОСТ 27.003 (п. 1.3). При этом важно понимать, что часть требований к модели эксплуатации по ГОСТ 27.003 в технических заданиях, формируемых по ГОСТ 34.602, излагаются в разделе «Требования к эксплуатации, техническому обслуживанию, ремонту и хранению».

Кроме того, перечень аварийных ситуаций может быть изложен для каждого периода эксплуатации системы (хранение, транспортирование, развертывание, ожидание применения по назначению, применение по назначению, техническое обслуживание и плановый ремонт) и влияют на сущность критериев отказов системы в целом.

В большей части применительно к АС на основе порталов (КПИ, УРСИ, РСИ[13] и других) перечень аварийных ситуаций приводится по компонентам системы:

i. *сбой общего или специального ПО (отдельного АРМ или сервера);*
ii. *выход из строя части КТС;*
iii. *сбои или выход из строя активного накопителя на жестком магнитном диске;*
iv. *ошибки персонала при работе с Системой;*
v. *импульсные помехи, сбои или прекращение электропитания.*

Последний пункт имеет отношение к обеспечению системы электропитанием и является типичным.

Важное замечание:

требования по надежности должны «покрываться» соответствующими техническими решениями и должны найти отражение в документах технического проекта:

---

[12] Как правило, рассматривают ТО следующих видов: годовое, полугодовое, ежемесячное, еженедельное и др.

[13] Совокупность информационных систем, разработанных по договорам с Банкам России.

- Пояснительной записке;
- Описание и схеме структурной КТС;
- Описании ПО;
- Спецификации в части используемых разновидностей (типов, видов) лицензий[14] на ПО и состава оборудования и программных средств.

4. Требования по надежности технических средств и программного обеспечения

В общем случае требования по надежности технических средств и программного обеспечения могут быть заданы по подсистемам. В простейшем случае задают общие требования к системе в целом. Такой вариант задания требований типичен для систем, подсистемы которой функционируют на одних и тех же аппаратных средствах, и, зачастую, посредством одного и того же ПО. Пример: проекты региональных сегментов Интранет Банка России.

В этом случае требования по надежности к ТС и ПО излагаются в соответствии с перечнем аварийных ситуаций (см. соответствующие ТЗ). Собственно это требования к ТС и ПО, соответствие которым обеспечило бы выход или недопущение указанных аварийных ситуаций.

5. Требования к методам оценки и контроля показателей надежности на разных стадиях создания системы в соответствии с действующими нормативно-техническими документами

Данный пункт ТЗ логичен в случае, когда предварительно указаны критерии выхода из строя системы (признак или набор признаков, по которым делается вывод о неработоспособности системы в целом). Более того, разработка каких-либо методик – суть разработка методического обеспечения системы, что требует дополнительных трудозатрат. Разработка методического обеспечения должна быть предусмотрена рамками проекта, сметой и т.д.

При отсутствии критериев, как правило, данный пункт ТЗ опускают.

При наличии критериев отказа, а соответственно и показателей надежности[15],

[14] Примером важности различных видов лицензий является проекты по региональным сегментам Интранет Банка России на основе MS SharePoint Portal Server 2003. Политика MS в области лицензирования предполагает использование программы Software Assurance (SA), в соответствии с которой кроме прочих преимуществ по каждой серверной лицензии можно было установить два экземпляра серверного ПО на два различных аппаратных сервера, один из которых используется в качестве холодного резерва.

[15] Под критерием в данном случае понимается показатель с примененным к нему каким-либо правилом. Например, под критерием отказа системы в целом можно понимать следующие: выход из строя более одной подсистемы; выход из строя всех серверов (основных и резервных); выход из строя только основных серверов и т.д. Показателем является количество вышедших из строя элементов, а правилом следующее: если превышает указанное количество подсистем (серверов и т.д.), то система считается вышедшей из строя.

системы или ее подсистем, методы (методики), должны позволять делать соответствующие оценки, как расчетным путем на этапах проектирования, так и расчетно-экспериментальным путем на этапах испытаний.

Суть логики такова:

- излагаются показатели надежности;
- излагаются критерии отказа (отказов), в которых в каком-либо виде присутствуют показатели надежности;

Дальнейший логический ход предполагает наличие методов или методик оценки, как показателей, так и критериев. Поскольку на этапе разработки ТЗ на систему эти методики отсутствуют, то имеет смысл изложить в нем требования к соответствующим методам.

Типичные примеры критериев отказов и предельных состояний изложены ниже в п.7.

При наличии соответствующих методик на этапе разработки ТЗ они должны быть изложены в нормативно-технических документах, которые должны быть согласованы с Заказчиком. В данном случае формулировку таких требований целесообразно изложить с указанием на эти документы.

Кроме всего прочего в методиках, основанных на расчетно-экспериментальных способах оценки, должны быть обоснованы временные рамки проведения испытаний, в пределах которых производится оценка показателей надежности. В простейшем случае, при выборе показателей надежности по п. 2 настоящего документа и с учетом высокого уровня надежности современной вычислительной техники, для оценки времени наработки на отказ T_o может потребоваться значительное время.

Например, при требуемом Заказчиком среднем времени восстановления АС $T_B \leq 3$ час и при коэффициенте готовности $K_Г \geq 0{,}999$, среднее время наработки на отказ системы составит $T_o \geq 3000$ час или не менее 125 суток в среднем. Таким образом, для проверки надежности системы минимальное время испытаний должно составить не менее 4 месяцев. Из этого следует, что проведение подобных проверок возможно только во время опытной эксплуатации, что и должно быть предусмотрено в соответствующей программе[16] (Программа опытной эксплуатации).

6. Взаимосвязь требования по надежности и других требований ТЗ

В следующей таблице показаны требования (пункты ТЗ в соответствии с ГОСТ 34.602), которые могут иметь связь (взаимное влияние) с требованиями по надежности. В любом случае изменения в данных пунктах ТЗ должны быть проверены на степень взаимного влияния этих изменений на требования по надежности, в особенности на количественные значения показателей надежности. Список представленных требований такого рода не может быть полным и в каждом конкретном случае (для конкретной АС) должен быть определен отдельно.

Таблица 2. Пункты ТЗ на АС, связанные с требованиями по надежности

Раздел	Подраздел ТЗ	Пункт ТЗ	Подпункт ТЗ	Влияние на	Связь с

[16] В соответствии с ГОСТ 34.603-92 проверка надежности и устойчивости функционирования программных и технических средств должна быть произведена во время проведения предварительных автономных испытаний. Однако проверка надежности всей системы в целом возможна только на комплексных или последующих испытаниях.

ТЗ				**требования по надежности**	**требованиями по ГОСТ 27.003**
4. Требования к системе	4.1.Требования к системе в целом	4.1.1.Требования к структуре и функционированию системы	4.1.1.4.Требования к режимам функционирования	Влияет на модель эксплуатации АС, что в свою очередь может повлиять на выбор (состав) показателей надежности	Типовая модель эксплуатации
			4.1.1.5.Требования по диагностированию системы	Методы (способы) диагностирования могут оказать влияние на время восстановления АС или ее частей (компонент)	Требования и (или) ограничения по конструктивным, технологическим и эксплуатационным способам обеспечения надежности, при необходимости, с учетом экономических ограничений
		4.1.8.Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы	4.1.8.1.Условия и регламент (режим) эксплуатации, которые должны обеспечивать использование технических средств (ТС) системы с заданными техническими показателями, в том числе виды и периодичность обслуживания ТС системы или допустимость работы без обслуживания;	Влияет на модель эксплуатации АС, что в свою очередь может повлиять на выбор (состав) показателей надежности	
			4.1.8.3.Требования по количеству, квалификации обслуживающего персонала и режимам его работы;	Количество и квалификация персонала может оказать влияние на качество проведения ТО и эксплуатации АС. Кроме того, на время восстановления (в этих требованиях следует указать, что должен знать и что уметь обслуживающий	

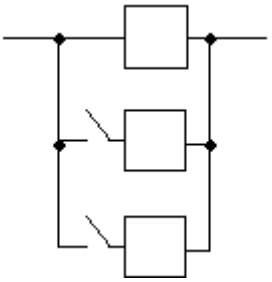
				персонал)	
			4.1.8.4.Требования к составу, размещению и условиям хранения комплекта запасных изделий и приборов (ЗИП).	Данные требования следует указать при необходимости наличия ЗИП. Влияет на время восстановления АС	Требования и (или) ограничения по конструктивным, технологическим и эксплуатационным способам обеспечения надежности, при необходимости, с учетом экономических ограничений в части ЗИП
			4.1.8.5.Требования к регламенту обслуживания.	Сроки, виды и периодичность ТО. Влияет на выбор (состав) показателей надежности.	
	4.2.Требования к функциям (задачам), выполняемым системой	4.2.5. Перечень и критерии отказов для каждой функции, по которой задаются требования по надежности.		Данные требования указываются при необходимости. В общем случае требования по надежности могут быть предъявлены к системе, к подсистемам, к отдельным задачам (функциям). Во всех случаях это должно найти свое отражение в требованиях по надежности.	Номенклатура и значения показателей надежности (ПН).
6.Порядок контроля и приемки системы	6.1.Виды, состав, объем и методы испытаний системы и ее составных частей (виды испытаний в соответствии с действующими нормами, распространяющимися на разрабатываемую			Влияет на состав и суть методического обеспечения. На проектных стадиях используются расчетные, а при испытаниях расчетно-экспериментальные методики оценки показателей надежности.	Методы контроля соответствия изделий заданным требованиям по надежности (контроля надежности)

	систему)				

Отдельно имеет смысл рассмотреть требования, предъявляемые к изделиям (по ГОСТ 27.003-90) по надежности в части конструктивных, технологических и эксплуатационных способов обеспечения надежности, поскольку часть из них находят свое отражение в других разделах ТЗ на АС, в частности в требованиях к техническому и программному обеспечений. В следующей таблице приведены возможные связи требований к конструктивным способам обеспечения надежности и разделов (пунктов) ТЗ на АС.

Таблица 3. Связь требования к конструктивным способам обеспечения надежности с разделами ТЗ на АС.

Требования по ГОСТ 27.003		Разделы (пункты) ТЗ на АС по ГОСТ 34.602
Требования к конструктивным способам обеспечения надежности могут содержать:		
	Требования и (или) ограничения по видам и кратности резервирования	Виды резервирования («горячее», «холодное») могут быть определены в пункте 4.1.4 «Требования к надежности», в п. 4.1.4.3 «Требования к надежности технических средств и программного обеспечения». Вид резервирования в основном определяется временем восстановления системы. Кратность резервирования определяет степень избыточности оборудования и лицензий на соответствующее ПО. Если: n – число однотипных элементов в системе; r – число элементов, необходимых для функционирования системы. Кратность резервирования – это соотношение между общим числом однотипных элементов и элементов, необходимых для работы системы: $k = (n - r)/r.$ Кратность резервирования может быть целой, если r=1, или дробной, если r>1. Например: i. для системы из трех элементов (см. рисунок ниже): $r=1$, $k=(3 - 1)/1 = 2,$ кратность резервирования k=2, что означает наличие двух резервных элементов (комплектов аппаратуры);

		 ii. для такого же количества элементов, но при r = 2, кратность резервирования k=0,5. Требования по кратности резервирования могут быть указаны в п. 4.1.4.3 «Требования к надежности технических средств и программного обеспечения», а также в разделах ТЗ, посвященных требованиям к техническому и программному обеспечений
	Требования и (или) ограничения по затратам (стоимости) в изготовлении и эксплуатации, массе, габаритам, объему изделия и (или) его отдельных составных частей, комплектов ЗИП, оборудования для технического обслуживания и ремонтов.	Как правило, к АС такого рода требования не предъявляются. Современные АС комплектуются закупаемыми техническими средствами промышленного производства, поэтому требования такого рода уже заложены в них производителями. Если такого рода ограничения (например, по габаритам – форм-фактор) имеются со стороны Заказчика, то их следует учитывать при выборе состава технических средств. Соответственно, эти требования указываются в разделе ТЗ «Требования к техническому обеспечению».
	Требования к структуре и составу ЗИП	Определяют виды запасных комплектующих (блоки питания, модули, платы и т.д.) и их состав и, возможно, количество. Данные требования следует излагать в п. 4.1.8.4. «Требования к составу, размещению и условиям хранения комплекта запасных изделий и приборов (ЗИП)».
	Требования к системе технического диагностирования (контроля технического состояния)	Излагаются в соответствующем пункте ТЗ 4.1.1.5. «Требования по диагностированию системы».
	Требования и (или) ограничения по способам и средствам обеспечения ремонтопригодности и сохраняемости	Данные требования предъявляются не к АС в целом, а к ее составляющим – аппаратным средствам. **Ремонтопригодность**[17] **-** свойство, заключающееся в приспособленности объекта (изделия) к поддержанию и восстановлению работоспособного состояния путем технического обслуживания и ремонта. Требования по ремонтопригодности предъявляются, как правило, к

[17] Основные стандарты, определяющие требования по ремонтопригодности:

- ГОСТ 27.002-89 Надежность в технике. Основные понятия. Термины и определения.
- ГОСТ 18322-78 Система технического обслуживания и ремонта техники. Термины и определения.
- ГОСТ 21623-76 Система технического обслуживания и ремонта техники. Показатели для оценки ремонтопригодности. Термины и определения.
- ГОСТ 23660-79 Система технического обслуживания и ремонта техники. Обеспечение ремонтопригодности при разработке изделий.
- ГОСТ 15.601-98 Система разработки и постановки продукции на производств. Техническое обслуживание и ремонт техники.

		восстанавливаемым изделиям. В качестве показателей ремонтопригодности используются: ■ время восстановления изделия, ■ трудозатраты на восстановления изделия. Требования по техническому обслуживанию и ремонту техники определены в ГОСТ 15.601-98. **Сохраняемость** – свойство объекта сохранять в заданных пределах значения параметров, характеризующих способности объекта выполнять требуемые функции, в течение и после хранения и (или) транспортирования. Также большей частью это требование относится к изделию (аппаратному средству) а не АС в целом. При необходимости указываются в пункте ТЗ 4.1.4.3. «Требования к надежности технических средств и программного обеспечения». Для АС, как правило, используются закупаемые аппаратные средства промышленного производства (не специально разработанные для конкретной АС)

7. Примеры типичных критериев отказов и предельных состояний

Примеры типичных критериев отказов и предельных состояний изложены в Приложение 6 к ГОСТ 27.003-90. Возможность использования данных критериев для АС на основе порталов изложена ниже (см. Таблица 4).

В общем случае критерии отказов следует формулировать на основании показателей эффективности, если эти показатели присутствуют в ТЗ. В случае, если показатели эффективности и само понятие эффективности никак не определены, то необходимо определить наиболее важные функции, выполняемые системой, либо характеристики (показатели, как количественные значения характеристик), выполнение или соблюдение которых свидетельствует о работоспособности системы.

Таблица 4. Типичные критерии отказов

№ п/п	Содержание критерия	Комментарий применимости для АС на основе порталов
1.	Прекращение выполнения изделием заданных функций; снижение качества функционирования (производительности, мощности, точности, чувствительности и других параметров) за пределы допустимого уровня	Возможные критерии отказов АС: 1. Возможно применения функционального критерия: прекращение выполнения одной или совокупности важных для заказчика функций. 2. Снижение производительности системы по обслуживанию заданного количества пользователей вследствие выхода из строя программных и аппаратных средств.
2.	Искажения информации (неправильные решения) на выходе изделий, имеющих и своем составе ЭВМ или другие устройства	Данный критерий применяется для систем, к которым предъявляются высокие требования по достоверности информации, например, для систем

	дискретной техники, из-за сбоев (отказов сбойного характера)	управления или АС, являющихся частью системы управления. Необходимость использования для АС на основе порталов данного критерия – маловероятно.
3.	Внешние проявления, свидетельствующие о наступлении или предпосылках наступления неработоспособного состояния (шум, стук в механических частях изделий, вибрация, перегрев, выделение химических веществ и т. п.)	Данный критерий более применим для аппаратных средств.

Формулировка критериев предельных состояний[18] должна быть согласована с формулировкой критериев отказа системы, и в лучшем случае отличаться только значениями конкретных параметров. Изложение критериев предельных состояний необходимо в случаях планирования ТО или ремонтных работ. Если ТО или ремонтные работы не предполагается планировать, то наличие критериев предельных состояний теряет смысл.

К типичному критерию предельных состояний для АС на основе порталов можно отнести:

i. отказ одной или нескольких составных частей (подсистем), восстановление или замена которых на месте эксплуатации не предусмотрена эксплуатационной документацией (должна выполняться в ремонтных органах);
ii. превышение установленного уровня текущих (суммарных) затрат на техническое обслуживание и ремонты или другие признаки, определяющие экономическую нецелесообразность дальнейшей эксплуатации.

Учитывая архитектуру АС на основе порталов, согласно которой, как правило, все или определенная совокупность функциональных подсистем строится на одном аппаратном сервере, то первый критерий предполагает выход из строя этого аппаратного средства (сервера) и соответствующих подсистем.

8. О программе обеспечения надежности

В соответствии с ГОСТ 27.002-89 под Программой обеспечения надежности (ПОН) понимают документ, устанавливающий комплекс взаимосвязанных организационно-технических требований и мероприятий, подлежащих проведению на определенных стадиях жизненного цикла объекта и направленных на обеспечение заданных требований к надежности и (или) на повышение надежности.

Программа обеспечения надежности - документ, служащий организационно-технической основой для создания систем, удовлетворяющих заданным требованиям по надежности. Программа должна охватывать все или отдельные стадии жизненного цикла объекта.

Программа обеспечения надежности включает, в частности, программу экспериментальной отработки, которая определяет цели, задачи, порядок проведения

[18] Под предельным понимается такое состояние, при достижении которого дальнейшая эксплуатация изделия (системы) нецелесообразна. В дальнейшем возможны ремонт, списание и т.д.

и необходимый объем испытаний или экспериментальной отработки, а также регламентирует порядок подтверждения показателей надежности на стадии разработки.

ПОН составляют для АСУ при разработке ТЗ и оформляют в виде отдельного организационно-распорядительного документа, являющегося приложением к ТЗ на АСУ. В обоснованных случаях допускают работы по обеспечению надежности АСУ включать в соответствующие разделы ТЗ, не составляя отдельного документа.

На необходимость разработки ПОН для АСУ указывает ГОСТ 24.701-86 (Надежность автоматизированных систем управления. Основные положения), а для средств вычислительной техники - ГОСТ 21552-84 (СВТ. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение).

В рамках ГОСТ 34.602 (для автоматизированных систем вообще) разработка ПОН не требуется в обязательном порядке. При необходимости (по условиям договора или так принято у Заказчика) ПОН приводят не виде отдельного документа, а в разделе технического задания под названием «Состав и содержание работ по созданию (развитию) системы». В этом разделе в обязательном порядке должен содержаться перечень стадий и этапов работ по созданию системы в соответствии с ГОСТ 24.601, сроки их выполнения, перечень организаций - исполнителей работ, ссылки на документы, подтверждающие согласие этих организаций на участие в создании системы, или запись, определяющую ответственного (заказчик или разработчик) за проведение этих работ.

Приложение А.

Вариант 1 требований по надежности к АС

4.1.4 Требования к надежности

4.1.4.1 Система должна относиться к обслуживаемым восстанавливаемым изделиям общего назначения многократного циклического применения согласно ГОСТ 27.003-90. Основные показатели надежности Системы согласно ГОСТ 24.701-86 и ГОСТ 27.003-90:

i. коэффициент готовности $K_г$ (вместо коэф. готовности можно указать среднее время наработки на отказ)[19];
ii. среднее время восстановления работоспособности $T_в$.

4.1.4.2 Аварийные ситуации, по которым регламентируются требования к показателям надежности Системы:

i. отказ любого программно-технического комплекса (ПТК) Системы в результате сбоя или выхода из строя его технических средств;
ii. отказ ПТК в результате сбоя его общего или специального программного обеспечения;
iii. сбой или отказ ПТК в результате ошибки в прикладном программном обеспечении (ППО) Системы;
iv. отказ канала связи Системы;

[19] Здесь далее цветом выделены формулировки, которые должны быть уточнены для конкретной системы

v. сбой или отказ ПТК в результате ошибки в работе персонала.

4.1.4.3 Количественные значения показателей надежности Системы должны быть не хуже следующих:

i. коэффициент готовности ПТК должен быть не менее <0,999> (или - среднее время наработки на отказ ПТК Системы должно составлять не менее <500> часов);
ii. коэффициент готовности канала связи должен быть не менее <0,99> (или - среднее время наработки на отказ канала связи Системы должно составлять не менее <300> часов);
iii. коэффициент готовности серверов Системы должен составлять не менее 0,9999 (или среднее время наработки на отказ серверов Системы должно составлять не менее <10000> часов);
iv. коэффициент готовности ПЭВМ в составе АРМ должен быть не менее 0,9999 (среднее время наработки на отказ ПЭВМ в составе АРМ должно составлять не менее <5000> часов);
v. среднее время наработки на отказ единичной функции ППО ПТК Системы должно составлять не менее 1500 часов;
vi. среднее время восстановления работоспособности ПТК Системы должно составлять не более <30> минут, при этом:
vii. среднее время восстановления работоспособности ПТК после отказов технических средств должно составлять - не более <20> минут, без учета времени организационных простоев;
viii. среднее время восстановления работоспособности ПТК после отказа общего или специального программного обеспечения Системы не более <20> минут без учета времени организационных простоев;
ix. среднее время восстановления работоспособности канала связи ПТК должно составлять не более <3> часов;
x. среднее время восстановления работоспособности ПТК в случае отказа или сбоя из-за алгоритмических ошибок прикладного программного обеспечения ПТК Системы, без устранения которых невозможно дальнейшее функционирование ПТК - до <8> часов (без учета времени на устранение ошибок).

Требования к характеристикам надежности не относятся к средствам, включенным в состав ПТК и Системы в целом или используемым ими, которые использовались в Системе на предыдущих этапах автоматизации.

Выполнение требований по количественным показателям надежности на этапе разработки Технического проекта Системы определяется расчетным путем.

Количественные значения показателей надежности уточняются по результатам опытной эксплуатации Системы.

4.1.4.4 Для ПТК Системы должно быть обеспечено резервирование средств вычислительной техники. Кратность резервирования определяется на этапе технического проекта.

4.1.4.5 ПТК считается работоспособным, если возможно решение не менее 50% его задач и выполнять функции в соответствии с его

назначением, вести обмен данными по ЛВС и каналам связи. Под отказом понимается любое другое состояние ПТК.

4.1.4.6 Для ПТК с учетом требований ГОСТ 21552-84 (п.1.4.1) должна быть разработана программа обеспечения надежности (ПОН).

4.1.4.7 ПОН должна включать следующие технические меры по обеспечению надежности ПТК Системы:

i. резервирование критически важных элементов и комплексов;
ii. использование технических средств с избыточными компонентами и возможностью их горячей замены;
iii. конфигурирование используемых технических средств.

4.1.4.8 ПОН должна включать следующие организационные меры по обеспечению надежности ПТК:

i. по минимизации ошибок персонала (пользователей), а также персонала службы эксплуатации при эксплуатации и проведении работ по обслуживанию Системы;
ii. по минимизации времени на устранение ошибок, внесение изменений и восстановление работоспособности ПТК и Системы в целом;
iii. по подготовке и порядку допуска к работе персонала (пользователей) требуемой квалификации, по организации его работы;
iv. по подготовке и порядку допуска к работе обслуживающего персонала требуемой квалификации, по организации его работы;
v. по обеспечению своевременной диагностики и устранению ошибок за счет использования специализированных программных средств, входящих в состав ПТК, ПТК мониторинга и управления;
vi. по формированию и порядку использования резервных копий прикладного программного обеспечения ПТК Системы, а также резервных копий информации, сохраняемой в ПТК 1-3 уровня;
vii. по сокращению времени организационных простоев в процессах устранения отказов и технического обслуживания программно-технических средств ПТК, в том числе по составу, принадлежности и оптимизации размещения ЗИП.

4.1.4.9 Гарантийный срок ПТК должен составлять не менее <2> лет. Гарантия не распространяется на средства, включенные в состав ПТК и Системы в целом или используемые ими, которые использовались Заказчиком на предыдущих этапах автоматизации его деятельности.

Приложение Б. Вариант 2 требований по надежности к АС

4.1.4 Требования к надежности

4.1.4.1 Перечень аварийных ситуаций

Возможны следующие аварийные ситуации:

i. сбой общего или специального ПО (отдельного АРМ или сервера);

ii. выход из строя части КТС;

iii. сбои или выход из строя активного накопителя на жестком магнитном диске;

iv. ошибки персонала при работе с Системой;

v. импульсные помехи, сбои или прекращение электропитания.

4.1.4.2 Сбой общего или специального ПО (отдельного АРМ или сервера)

После сбоя серверной операционной системы или СУБД, в процессе выполнения пользовательских задач, должно быть обеспечено восстановление данных до состояния на момент окончания последней нормально завершенной перед сбоем транзакции.

Время восстановления работоспособности при любых сбоях и отказах не должно превышать 3-х часов. В это значение входит разворачивание и настройка специального ПО на сервере, а также восстановление данных с использованием последней резервной копии. В указанное время не входит решение проблем с техническим обеспечением и инсталляция операционной системы.

Выход из строя одного из АРМ или нарушение канала связи локальной сети между АРМ и сервером не должны приводить к прекращению функционирования в целом всей Системы.

4.1.4.3 Сбои или выход из строя активного накопителя на жестком магнитном диске

Должна быть обеспечена возможность «горячей» замены сбойного или вышедшего из строя одного активного накопителя на жестком магнитном диске в составе дискового массива без остановки функционирования всей Системы и потерь информации.

Должна быть обеспечена возможность восстановления данных с внешнего накопителя после восстановления активного накопителя.

4.1.4.4 Ошибки персонала при работе с Системой

Система должна локализовать ошибки персонала при работе с Системой. Должны быть предусмотрены меры предотвращения

удаления активных системных файлов, а также предупреждения об удалении информационных ресурсов.

4.1.4.5 Импульсные помехи, сбои или прекращение электропитания

Импульсные помехи, сбои или прекращение электропитания не должны приводить к выходу из строя технических средств и/или нарушению целостности данных.

Время прекращение электропитания определяется возможностями системы резервного питания существующей <на объектах Заказчика>.

4.1.4.6 Требования к надежности технических средств и программного обеспечения

Надежность Системы должна обеспечиваться:

i. использованием ТС повышенной отказоустойчивости и их структурным резервированием;
ii. защитой ТС по электропитанию путем использования источников бесперебойного питания;
iii. дублированием носителей информационных массивов.

4.1.4.7 Назначенные сроки службы, среднее время наработки на отказ не устанавливаются, а определяются в соответствии с заявленными производителями характеристиками выбранных технических средств.