2015

**Требования к качеству функционирования информационных систем, используемых при предоставлении государственных и муниципальных услуг в электронной форме**

**Версия 1.0**

**08.09.2015**

# **Общие положения**

* 1. **Назначение документа**

Настоящий документ описывает требования к качеству функционирования информационных систем, используемых при предоставлении государственных и муниципальных услуг в электронной форме. Также в данном документе определяется методика определения уровня качества функционирования.

* 1. **Нормативные основания разработки документа**

Протокол заседания Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 3 июля 2015 г. №1

Данный документ разработан в том числе во исполнение:

* Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
* Постановления Правительства Российской Федерации от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия» (далее Постановление № 697);
  1. **Область действия**

Федеральные органы исполнительной власти, государственные внебюджетные фонды, региональные органы исполнительной власти и органы местного самоуправления, а также их подведомственные учреждения, являющиеся операторами информационных систем, используемых при предоставлении государственных и муниципальных услуг в электронной форме, в том числе при осуществлении электронного межведомственного взаимодействия в целях предоставлении государственных и муниципальных услуг (далее - Операторы ИС).

* 1. **Термины и определения:**

В документе используются следующие термины и определения:

|  |  |
| --- | --- |
| ИС | Информационная система |
| ИЭП | Инфраструктура электронного правительства |
| Артефакт | Проектные документы, рабочие документы, схемы, модели, диаграммы и прочая, описывающая работу и архитектуру ИС, документация |
| Валидация | процесс приведения доказательств того, что требования Оператора (Заказчика) по разработке или развитию ИС корректно удовлетворены |
| Верификация | процесс приведения доказательств того, что требования Технического задания (Спецификации) по разработке или развитию ИС корректно реализованы |
| Оператор СМЭВ | Министерство связи и массовых коммуникаций Российской Федерации (в соответствии с постановлением Правительства РФ N 697 от 08.09.2010) |
| Ситуационный центр | Интернет-ресурс, с помощью которого осуществляются коммуникации по вопросам получения или предоставления информационно-методической поддержки Участникам информационного  взаимодействия, доступный по адресу https://sc.minsvyaz.ru |
| Репозиторий исходного кода (система управления версиями) | Система хранения и управления изменения исходными кодами ИС |
| Статический анализ кода | Анализ (тестирование) программного обеспечения, производимый (в отличие от динамического анализа) без реального выполнения исследуемых программ |
| Процедура Проверка кода (Code Review) | Систематическая проверка исходного кода программы разработчиками с целью обнаружения и исправления ошибок, которые остались незамеченными в начальной фазе разработки. Целью просмотра является улучшение качества программного продукта и совершенствование навыков разработчиков |
| Процесс непрерывной интеграции исходных кодов | Практика разработки программного обеспечения, которая заключается в выполнении частых автоматизированных сборок проекта для скорейшего выявления и решения интеграционных проблем |
| Дефект исходного кода | Ошибка в программном обеспечении ИС |
| Масштабируемость ИС | Способность ИС справляться с увеличением рабочей нагрузки (увеличивать свою производительность) при добавлении аппаратных ресурсов |
| Ошибка | Ошибка обработки межведомственного запроса – факт некорректной обработки межведомственного запроса со стороны ИС поставщика сервиса, либо факт недоступности ИС поставщика сервиса в СМЭВ |
| ПО | Программное обеспечение |
| СМЭВ | Система межведомственного электронного взаимодействия |
| ПМИ | Программа и методика испытаний |
| ОИВ | Органы исполнительной власти |

# **Методика мониторинга качества функционирования Информационных систем**

Измерение качества функционирования информационных систем, используемых при предоставлении государственных и муниципальных услуг в электронной форме производится путем анализа Оператором СМЭВ записей логов СМЭВ на предмет наличия кодов событий, свидетельствующих о фактах ошибок.

Коды событий ошибок в логах СМЭВ:

* Ошибка вызова внешнего сервиса поставщика (код 1205) – ошибка на стороне сервиса ведомства
* Внешний сервис поставщика временно недоступен (код 1210) – сервис не отвечает в установленный таймаут
* Внешний сервис поставщика временно недоступен (код 1211) – сервис заблокирован служебным инструментом проверки доступности сервисов СМЭВ
* Сертификат ответа не действителен (код 1120) – ответ от ведомственного сервиса подписан не валидным сертификатом электронной подписи

Коды событий успешной обработки запросов в логах СМЭВ:

* Получено сообщение (код 1010) – сообщение от потребителя получено СМЭВ
* Сообщение доставлено поставщику (код 1080) - сообщение прошло проверки СМЭВ и отправлено ИС поставщика сервиса
* Сообщение получено от поставщика (код 1090) - ответ от поставщика сервиса получен СМЭВ
* Сообщение передано потребителю (код 1140) - ответ прошел проверки СМЭВ и отправлен ИС потребителя

На основании данных измерений определяется уровень качества функционирования информационных систем. Уровень качества высчитывается в процентах путем определения доли межведомственных запросов, обработанных с ошибкой, в общем объеме межведомственных запросов, направленных на сервисы данной ИС посредством СМЭВ за период измерений.

Дополнительно Оператором СМЭВ производится учет и обработка фактов ответов на межведомственные запросы, в которых предоставлены некорректные данные. Все подобные факты подлежат разбирательству и выяснению причин, а также планированию корректирующих действий.

Уровень качества определяется еженедельно Оператором СМЭВ. Измерения проводятся с 00:00:00 понедельника по 23:59:59 воскресения соответствующей отчетной недели. В статистическую выборку не принимаются периоды запланированных профилактических работ и работ по установке обновлений ИС поставщиков. Операторы ИС обязаны извещать оператора СМЭВ о планируемых профилактических работах и работах по установке обновлений посредством Ситуационного центра электронного правительства. Профилактические работы и работы по установке обновлений должны планироваться на периоды наименьшей востребованности ИС, в ночное время и в выходные дни. По факту завершения профилактики Оператор ИС направляет уведомление Оператору СМЭВ.

На основании данных еженедельного мониторинга качества определяется рейтинг уровня качества Операторов ИС. Рейтинг регулярно выносится на рассмотрение Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности.

# **Обязанности Операторов ИС**

Операторы ИС обязаны обеспечить качество функционирования информационных систем, используемых при предоставлении государственных и муниципальных услуг в электронной форме на уровне не более 1% ошибок от общего объема обработанных межведомственных запросов путем реализации требований по обеспечению требуемого уровня качества (п. 4 настоящего документа).

# **Требования по обеспечению требуемого уровня качества функционирования ИС**

* 1. **Обязательные требования:**

**Обязательные требования к составу мер по обеспечению качества функционирования ИС на стадии эксплуатации**

1. Обеспечение работы службы дежурных администраторов ИС. График работы службы администраторов, поддерживающих ИС, должен обеспечить возможность исполнения регламентных сроков реагирования и решения обращений (инцидентов) в соответствии с Приказом Министерства связи и массовых коммуникаций Российской Федерации от 1 июля 2014 г. N 184.
2. Своевременное реагирование на инциденты и запросы. Обращения, полученные посредством Ситуационного центра электронного правительства, должны обрабатываться в регламентные сроки, установленные Приказом Министерства связи и массовых коммуникаций Российской Федерации от 1 июля 2014 г. N 184. Обращения требующие эскалации на другое ведомство или на Оператора СМЭВ перенаправляются посредством Ситуационного центра электронного правительства.
3. Управление непрерывностью и доступностью ИС. Необходимо определить меры и процедуры обеспечения непрерывности работы и доступности ИС, в том числе процедуры создания и проверки резервных копий, проверки восстановления ИС после сбоев, создания регламентов действий служб поддержки в случаях аварийной ситуации, определения и внедрения архитектурных решений обеспечивающих большую доступность и непрерывность. Доступность ИС должна обеспечивать соблюдение требуемого уровня качества - не более 1% ошибок от общего объема обработанных межведомственных запросов.
4. Определение формализованной процедуры приемки создаваемых ИС и всех обновлений функционирующих ИС в эксплуатацию, процедура должна исключить приемку несанкционированных обновлений и учесть все требуемые мероприятия контроля качества.
5. Реализация функциональных возможностей самодиагностики и уведомления об ошибках в функционирующих ИС. Должны быть реализованы механизмы выявления ошибок и аварий в функционирующих ИС, в том числе инструменты уведомления служб поддержки.
6. Определение формализованной процедуры (регламента) управления изменениями в эксплуатируемых ИС. Регламент должен определять правила приемки изменений функционирующих ИС в эксплуатацию, классификацию изменений по масштабу и срочности, состав процедур проверок и тестирования для каждого класса изменений, порядок действий по откату изменений.

**Обязательные требования к составу мер по обеспечению качества функционирования ИС на стадии разработки**

1. Разделение сред. Среды разработки тестирования и эксплуатации должны быть разделены на физическом и логическом уровнях инфраструктуры.
2. Функциональное тестирование. Все изменения эксплуатируемых ИС должны проходить процедуру функционального тестирования на тестовой и продуктивной среде. Функциональное тестирование предполагает проверку новых и измененных функциональных модулей на работоспособность и соответствие спецификации.
3. Регрессионное тестирование. Все изменения эксплуатируемых ИС должны проходить процедуру регрессионного тестирования на тестовой и продуктивной среде с целью контроля влияния нового функционала на работу существующей системы. Рекомендуется автоматизация основных регрессионных тестов.
   1. **Дополнительные требования:**

**Дополнительные требования к составу мер по обеспечению качества функционирования ИС на стадии эксплуатации**

1. Пилотные зоны опытной эксплуатации. Существенные изменения в функционирующих системах рекомендуется по возможности апробировать в ограниченных зонах пилотной эксплуатации перед тиражированием на полный объем пользователей.
2. Вывод из эксплуатации. Рекомендуется определить формализованную процедуру вывода ИС, либо ее компонентов или сервисов из эксплуатации, предусмотрев меры по уведомлению потребителей сервисов, бесперебойной замены компонентов, предоставляющих сервисы.
3. Обеспечение резервирования. Рекомендуется в инфраструктуре ИС предусмотреть резервирование ключевых компонентов с целью повышения отказоустойчивости ИС.
4. Обеспечения процедуры резервного копирования. Рекомендуется обеспечить выстраивание формализованного процесса управления резервными копиями ИС, включающего правила создания хранения и проверки резервных копий, а также регламенты восстановления и уничтожения резервных копий.

**Дополнительные требования к составу мер по обеспечению качества функционирования ИС на стадии разработки**

1. Организация процесса управления требованиями к разрабатываемым информационным системам. Рекомендуется выстраивание обеспечить формализованного процесса управления функциональными и нефункциональными требованиями, включающего стадии постановки высокоуровневых требований, их уточнения, классификации и приоритезации, трассировки (отслеживания) на всех стадиях проектирования и реализации функциональных и нефункциональных возможностей ИС. Данный процесс должен позволить обеспечить:
   1. Контроль верификации и валидации требований на всех уровнях детализации;
   2. Отсутствие противоречий между требованиями;
   3. Контроль полного покрытия «бизнес-требований» функциональными и нефункциональными требованиями в проектной документации;
   4. Контроль наличия всех необходимых видов тестов и тестовых сценариев в составе Программы и методики испытаний (ПМИ);
   5. Формирование полноценной спецификации ИС.

Рекомендуется применение специализированных инструментов, автоматизирующих процесс управления требованиями.

1. Обеспечение и контроль качества кода. Рекомендуется вводить в процесс разработки процедуры обеспечения и контроля качества кода такие как:

-Создание централизованного репозитория исходного кода и используемых артефактов;

-Определение правил проверки кода при помещении в репозиторий;

-Статический анализ кода;

-Процедура Проверка кода (Code Review);

-Процесс непрерывной интеграции исходных кодов.

1. Контроль исходных кодов на предмет дефектов (уязвимостей) информационной безопасности. Рекомендуется ввести в процесс разработки обязательную процедуру автоматизированного контроля исходного кода на уязвимости.
2. Модульное тестирование. Практика встраивания модульных (компонентных) тестов в исходные коды. Рекомендуется обязательным требованием к организации процесса разработки определить покрытие исходных кодов модульными тестами и процедуру их проведения до и во время сборки.
3. Системное тестирование. Рекомендуется в процесс приемки в эксплуатацию разработанного программного обеспечения, соответственно и в ПМИ, включать различные виды системного тестирования:

-Функциональное тестирование. Проверка соответствия разработанного программного обеспечения функциональным требованиям технического задания (спецификации). Рекомендуется автоматизировать основные функциональные тесты для применения в целях регрессионного тестирования;

-Интеграционное тестирование. Проверка корректности взаимодействия системы с другими внешними и внутренними системами и сервисами;

-Нагрузочное тестирование. Проверка работоспособности ИС под прогнозируемой нагрузкой, выявление дефектов и проблем производительности ИС;

-Тестирование уровня защищенности с точки зрения информационной безопасности.

1. Тестовые пользователи. Рекомендуется предусмотреть возможность применения тестовых учетных записей пользователей, запросы от которых будут корректно распознаваться ИС и не приниматься в продуктивный сценарий работы.
2. Масштабируемая архитектура. Рекомендуется при определении архитектуры разрабатываемой ИС закладывать требования к высокой способности динамического масштабирования для увеличения производительности ИС соответственно выделяемым вычислительным ресурсам.