ГОСТ 34009-2016

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

СРЕДСТВА И СИСТЕМЫ УПРАВЛЕНИЯ ЖЕЛЕЗНОДОРОЖНЫМ ТЯГОВЫМ ПОДВИЖНЫМ СОСТАВОМ

Требования к программному обеспечению

Control devices and systems for railway traction rolling stock. Software requirements

МКС 35.080
45.060

Дата введения 2017-08-01

Предисловие

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации установлены в ГОСТ 1.0-2015 "Межгосударственная система стандартизации. Основные положения" и ГОСТ 1.2-2015 "Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Порядок разработки, принятия, обновления и отмены"

Сведения о стандарте

1 РАЗРАБОТАН Закрытым акционерным обществом "ИБТранс" (ЗАО "ИБТранс")

2 ВНЕСЕН Межгосударственным техническим комитетом по стандартизации МТК 524 "Железнодорожный транспорт"

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 22 ноября 2016 г. N 93-П)

За принятие проголосовали:

Краткое наименование страны по МП* (ИСО 3166) 004-97	Код страны по МК (ИСО 3166) 004-97	Сокращенное наименование национального органа по стандартизации
Армения	AM	Минэкономики Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Таджикистан	TJ	Таджикстандарт

Украина	UA	Минэкономразвития Украины

_____

* Вероятно ошибка оригинала. Следует читать: МК. - Примечание изготовителя базы данных.

4 Приказом Федерального агентства по техническому регулированию и метрологии от 11 января 2017 г. N 3-ст межгосударственный стандарт ГОСТ 34009-2016 введен в действие в качестве национального стандарта Российской Федерации с 1 августа 2017 г.

5 ВВЕДЕН ВПЕРВЫЕ

6 Пункты 4.2-4.7; 7.1, 7.2; 9.2, 9.5, 9.6, 9.14, 9.21, 9.22 настоящего стандарта могут быть использованы для подтверждения соответствия требованиям безопасности, установленным нормативно-правовыми актами в области технического регулирования

Информация об изменениях к настоящему стандарту публикуется в ежегодном информационном указателе "Национальные стандарты" (по состоянию на 1 января текущего года), а текст изменений и поправок - в ежемесячном информационном указателе "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе "Национальные стандарты". Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

1 Область применения

Настоящий стандарт устанавливает требования к встроенному и прикладному программному обеспечению бортовых систем управления железнодорожным тяговым подвижным составом, в том числе высокоскоростным железнодорожным подвижным составом.

Настоящий стандарт применяют при разработке, производстве, эксплуатации и оценке соответствия программного обеспечения средств и систем управления тяговым подвижным составом.

Настоящий стандарт предназначен для заказчиков, поставщиков, разработчиков, потребителей, органов по сертификации, а также персонала сопровождения программного обеспечения средств и систем управления тяговым подвижным составом и систем управления тяговым подвижным составом в целом.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 15.902-2014 Система разработки и постановки продукции на производство. Железнодорожный подвижной состав. Порядок разработки и постановки на производство

ГОСТ 19.201-78 Единая система программной документации. Техническое задание. Требования к содержанию и оформлению

ГОСТ 19.202-78 Единая система программной документации. Спецификация. Требования к содержанию и оформлению

ГОСТ 19.401-2000[1)] Единая система программной документации. Текст программы. Требования к содержанию, оформлению и контролю качества

_____

[1)] В Российской Федерации действует ГОСТ 19.401-78 "Единая система программной документации. Текст программы. Требования к содержанию и оформлению".

ГОСТ 19.501-78 Единая система программной документации. Формуляр. Требования к содержанию и оформлению

ГОСТ 19.503-79 Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению

ГОСТ 19.505-79 Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению

ГОСТ 33432-2015 Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта

ГОСТ 33433-2015 Безопасность функциональная. Управление рисками на железнодорожном транспорте

Примечание - При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю "Национальные стандарты", который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя "Национальные стандарты" за текущий год. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **программное обеспечение (средств и систем управления тяговым подвижным составом); ПО ТПС:** Совокупность программных модулей для выполнения функций управления единицей тягового подвижного состава, встроенного программного обеспечения реального времени средств управления и программных документов, необходимых для их эксплуатации.

3.2 **система управления тяговым подвижным составом**: Комплекс бортового электромеханического и электронного оборудования, предназначенный для управления и контроля режимов движения единицы тягового подвижного состава, а также обеспечения безопасности движения поездов.

3.3 **прикладное программное обеспечение**: Часть программного обеспечения системы управления тяговым подвижным составом, которая обеспечивает выполнение определенных прикладных задач и функций управления, контроля и безопасности и рассчитана на непосредственное взаимодействие с пользователем.

3.4 **встроенное программное обеспечение**: Программное обеспечение (микропрограмма), записанное в энергонезависимой памяти электронного устройства и неотделимое от аппаратного обеспечения.

3.5

тяговый (железнодорожный) подвижной состав; ТПС: Совокупность видов железнодорожного подвижного состава, обладающего тяговыми свойствами для выполнения перевозочного процесса и включающая в себя локомотивы и моторвагонный подвижной состав.

[ГОСТ 31539-2012, статья 3]

3.6 **заказчик:** Предприятие (организация, объединение или другой субъект хозяйственной деятельности), по заявке или договору с которым производится создание и (или) поставка программного обеспечения средств и систем управления тяговым подвижным составом.

3.7 **несанкционированный доступ:** Доступ к информации, нарушающий правила разграничения доступа.

3.8 **недекларированные возможности:** Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации на него, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

3.9 **функциональная безопасность (системы управления тяговым подвижным составом):** Свойство системы управления тяговым подвижным составом выполнять требуемые функции безопасности при всех предусмотренных условиях в течение заданного периода времени.

3.10 **сбой (программного обеспечения)**: Самоустраняющийся отказ или однократный отказ, устраняемый вмешательством оператора.

3.11 **версия программного обеспечения**: Идентифицированное надлежащим образом программное обеспечение определенной конфигурации в конкретный момент времени.

3.12 **полнота безопасности программного обеспечения**: Составляющая полноты безопасности системы управления тяговым подвижным составом, касающаяся систематических отказов, проявляющихся как опасные отказы и относящихся к программному обеспечению.

3.13 **уровень полноты безопасности программного обеспечения**; УПБ: дискретный уровень (принимающий одно из четырех возможных значений от 1 до 4), определяющий полноту безопасности программного обеспечения системы, связанной с безопасностью.

3.14 **киберзащищенность программного обеспечения:** Безопасное состояние программного обеспечения, позволяющее выполнять предусмотренные задачи в условиях деструктивных воздействий с использованием инфраструктуры или элементов киберпространства, возникновения технологических нарушений и/или отказов технических средств.

Примечание - Киберпространство - это среда информационного взаимодействия и обмена данными, реализуемая в компьютерных сетях и сетях связи. Элементами киберпространства являются серверы, компьютеры, телекоммуникационное оборудование, каналы связи, информационные и телекоммуникационные сети.

3.15 **защитная мера**: Мера, предпринимаемая для снижения риска разработчиком или пользователем.

3.16 **эталонный носитель (программного обеспечения)**: Запоминающее электронное устройство, в память которого загружено программное обеспечение, идентифицированное надлежащим образом с помощью контрольной суммы (с указанием метода ее получения).

Примечание - Под контрольной суммой понимают число, рассчитанное путем проведения определенных операций над входными данными (например, хэш-сумма, электронная цифровая подпись).

4 Общие требования

4.1 ПО ТПС должно удовлетворять требованиям технического задания (частного технического задания) на ПО ТПС и выполнять все заданные для ПО функции системы управления единицей ТПС.

4.2 ПО ТПС, как встраиваемое, так и поставляемое на электронных носителях информации, в соответствии с техническим заданием (частным техническим заданием) должно:

а) обеспечивать выполнение всех предусмотренных техническим заданием функций управления, контроля и безопасности;

б) обеспечивать тестируемость и диагностику оборудования и компонентов бортовых систем единицы ТПС;

в) обеспечивать контроль целостности программ и данных;

г) обеспечивать нахождение в работоспособном состоянии после перезагрузок, вызванных сбоями и (или) отказами технических средств, и целостность при собственных сбоях;

д) быть защищено от компьютерных вирусов и несанкционированного доступа (см. раздел 7);

е) быть защищено от последствий отказов, ошибок и сбоев при хранении, вводе, обработке и выводе информации, от возможности случайных изменений информации;

ж) соответствовать свойствам и характеристикам, описанным в сопроводительной документации;

и) обеспечивать возможность определения предотказного состояния единицы ТПС по данным от информационных датчиков единицы ТПС с последующим сохранением информации о событии в электронной базе ПО ТПС;

к) обеспечивать проведение предрейсового контроля технического состояния единицы ТПС с информированием о месте и причине отказа в работе оборудования;

л) иметь интуитивно-понятный интерфейс взаимодействия с системой "человек-машина".

В ПО ТПС должны отсутствовать недекларированные возможности[1)].

[1)] Факт структурно-логического соответствия реальных и декларируемых возможностей программного обеспечения устанавливают по результатам анализа исходных текстов программ с помощью инструментальных программных средств и изучения текстов программ экспертами.

4.3 ПО ТПС должно обеспечивать контроль установленных скоростей движения, периодическую проверку бдительности машиниста, препятствовать самопроизвольному уходу поезда с места его стоянки и обеспечивать автоматическую остановку поезда в предусмотренных нештатных ситуациях и не должно допускать изменений и режимов работы, которые могут привести к нарушению безопасного состояния единицы ТПС.

ПО ТПС должно обеспечивать управление работой тягового привода и вспомогательного оборудования при возникновении неисправности аппаратов электрической, гидравлической и (или) пневматической составных частей без нарушения режимов работы, которые могут привести к нарушению безопасного состояния единицы ТПС.

4.4 ПО ТПС должно удовлетворять требованиям функциональной безопасности, предъявляемым в соответствии с [1]. На основе результатов оценки рисков (см. 6.7) устанавливают уровень полноты безопасности (далее - УПБ) для отдельных функций, системы управления единицей ТПС в целом и ПО ТПС, как составной части системы. Рекомендуемые УПБ для видов функций, реализуемых ПО ТПС, приведены в таблице 1.

Таблица 1 - Рекомендуемые УПБ для видов функций, реализуемых ПО ТПС

Функции, реализуемые ПО ТПС	Рекомендуемый УПБ, не ниже
Для магистральных локомотивов, моторвагонного подвижного состава и специального самоходного подвижного состава, предназначенных для движения со скоростью до 200 км/ч:	
- функции управления и контроля единицы ТПС	УПБ 1
- функции торможения (кроме экстренного торможения)	УПБ 2
- функции безопасности (в том числе функции, связанные с реализацией экстренного торможения, контроля бдительности машиниста и т.п.)	УПБ 3
- функции управления внешними пассажирскими дверями	УПБ 2
Для маневровых локомотивов:	
- функции управления и контроля единицы ТПС	УПБ 1
- функции маневровой автоматической локомотивной сигнализации	УПБ 2
Для высокоскоростного подвижного состава:	
- функции управления и контроля единицы ТПС	УПБ 2
- функции безопасности	УПБ 4
- функции управления внешними пассажирскими дверями	УПБ 2

4.5 Сбой ПО ТПС при исправной работе бортовых устройств безопасности не должен приводить к остановке и нарушению функционирования единицы ТПС.

4.6 Время, необходимое для перезагрузки отдельных систем управления следует задавать на стадии технического проекта. Необходимость перезапуска ПО ТПС должна допускаться только в исключительных случаях (как правило, при отказах аппаратного обеспечения). Каждый перезапуск системы должен регистрироваться в записывающем устройстве. Перезапуск системы управления единицей ТПС не должен влиять на:

- функции управления тормозами, влияющие непосредственно на тормозную магистраль;

- функции, отвечающие за безопасность, реализованные непосредственно аппаратным оборудованием.

4.7 В случае возникновения отказов ПО ТПС должны генерировать диагностические сообщения, которые должны сохраняться в памяти и при помощи текста выводиться у машиниста на дисплее.

4.8 В системе управления единицей ТПС должна быть установлена версия ПО ТПС, соответствующая версии, указанной в декларации о соответствии требованиям безопасности на ПО ТПС.

4.9 Набор показателей, обеспечивающих выполнение требований к качеству ПО ТПС, которые влияют на безопасность, приведены в приложении А, таблица А.1.

4.10 ПО ТПС должно соответствовать требованиям киберзащищенности, установленным национальными нормативными документами государств, применяющих настоящий стандарт.

5 Требования к документации

5.1 Основным документом, содержащим требования к ПО ТПС, является техническое задание на ПО ТПС или частное техническое задание на ПО ТПС в рамках технического задания на систему управления единицей ТПС в целом, разрабатываемые по ГОСТ 19.201.

Для ПО ТПС иностранного производства вместо технического задания (частного технического задания) допускается использование документа "спецификация требований" в соответствии с международной по [1] и европейской по [2] практиками.

5.2 Рабочие (проектные) документы ПО ТПС должны определять:

- структуру и содержание исходных и отчетных документов по стадиям разработки, испытаний и сопровождения ПО ТПС;

- логическую структуру программных компонентов и баз данных;

- спецификации требований на внутренние межмодульные интерфейсы компонентов ПО ТПС и на интерфейсы с внешней средой;

- язык и правила программирования, идентификации компонентов, комментирования текстов программ и описаний данных;

- методы тестирования, испытаний и аттестации программных компонентов и ПО ТПС в целом;

- порядок внесения изменений в ПО ТПС;

- оформление, форматы и обозначения отчетных документов.

5.3 Эксплуатационные документы должны исключать возможность некорректного использования ПО ТПС за пределами условий эксплуатации, при которых документами гарантируются определенные характеристики качества функционирования программ.

Эксплуатационная документация включает в себя:

- руководства пользователей, осуществляющих установку и непосредственное управление режимами решения функциональных задач, регламентированными в системе управления единицей ТПС (например, руководство системного программиста по ГОСТ 19.503);

- руководства пользователей, применяющих ПО ТПС по прямому назначению (например, руководство оператора по ГОСТ 19.505 для машиниста);

- руководство по установке ПО ТПС;

- документацию сопровождения ПО ТПС, формуляр.

5.4 Обязательными для ПО ТПС являются следующие документы:

- текст программы (описание файловой структуры) по ГОСТ 19.401;

- текст программы на исходном языке, если это оговорено в договоре на поставку;

- спецификация по ГОСТ 19.202;

- формуляр ПО ТПС по ГОСТ 19.501;

- программа обеспечения безопасности по ГОСТ 33432;

- доказательство безопасности по ГОСТ 33432;

- руководства пользователей.

6 Требования к процессам создания программного обеспечения

6.1 При создании ПО ТПС целесообразно учитывать:

- необходимость проектирования отдельных модулей таким образом, чтобы удовлетворить индивидуальным требованиям применения на конкретных видах ТПС,

- что системы управления единицей ТПС, как правило, являются системами реального времени, в которых преимущественно используют встроенное программное обеспечение.

6.2 Разработка и сопровождение ПО ТПС включает в себя:

- определение требований к ПО ТПС и разработку технического задания;

- разработку и проектирование архитектуры ПО ТПС;

- проектирование и кодирование программных модулей и программного обеспечения реального времени;

- интеграцию программных модулей и программного обеспечения реального времени;

- тестирование ПО ТПС;

- интеграцию и валидацию системы управления единицей ТПС в целом;

- сопровождение и модификацию ПО ТПС.

Особенности сопровождения и модификации ПО ТПС, влияющие на безопасность, приведены в разделе 9.

6.3 Установление требований к ПО ТПС осуществляют на основе анализа требований к системе управления ТПС.

При установлении требований к ПО ТПС необходимо отразить следующие аспекты для каждого компонента ПО ТПС:

- функциональные возможности, включая характеристики производительности и среды функционирования компонента;

- требования к внешним интерфейсам;

- спецификация требований (функциональной) безопасности, включающая требования к функциям безопасности и требования к полноте безопасности ПО ТПС по отношению к систематическим отказам (задание УПБ программного обеспечения) в соответствии с [1];

- эргономические требования;

- требования к используемым данным;

- требования к установке и приемке;

- требования к документации пользователей;

- требования к эксплуатации и сопровождению;

- требования к обеспечению киберзащищенности (при необходимости).

Требования к ПО ТПС оценивают исходя из критериев их соответствия требованиям к системе управления единицей ТПС, реализуемости и возможности проверки при тестировании.

6.4 Требования к ПО ТПС иерархически распределяют по всем подчиненным частичным функциям.

Все функции должны быть реализованы с расчетом на максимально возможную отказоустойчивость, должны быть учтены заданные рабочие состояния единицы ТПС, а также возможные отказы и неисправности устройств системы управления единицей ТПС и управляемого ею оборудования единицы ТПС.

6.5 Должна быть определена защитная стратегия, которая позволила бы локализовать сбои и защитить ПО ТПС от сбоев. При установлении возможных сбоев должна быть согласована процедура действий для восстановления или обеспечения работоспособного и безопасного состояния системы управления единицей ТПС. Защитная стратегия должна быть документирована и проверена.

6.6 Должны быть приняты меры против ложного срабатывания средств управления из-за влияния различных помех. Ложные команды системы управления единицей ТПС должны быть обнаружены и должна быть обеспечена возможность их блокировки.

6.7 В рамках проведения анализа требований к системе управления единицей ТПС и анализа риска для нее, из совокупности опасностей для системы управления единицей ТПС в целом должны быть выделены опасности и угрозы для ПО ТПС, включая угрозы информационной, функциональной безопасности и угрозы, связанные с киберзащищенностью. По результатам формируют протокол угроз.

Протокол угроз оформляют аналогично журналу учета опасностей по ГОСТ 33433-2015, пункт 6.2.5.

Если риски для выявленных угроз превышают допустимый уровень риска, то они должны быть снижены посредством применения различных защитных мер.

Общий процесс менеджмента риска для программного обеспечения в соответствии с [3] особенности менеджмента риска для угроз информационной безопасности по [4].

6.8 Разработка архитектуры ПО ТПС включает в себя следующие задачи (для каждого компонента ПО ТПС):

- трансформацию требований к ПО ТПС в архитектуру, определяющую на высоком уровне структуру ПО ТПС и состав его компонентов;

- разработку и документирование программных интерфейсов ПО ТПС и баз данных;

- разработку предварительной версии документации пользователей;

- разработку предварительных плана интеграции ПО ТПС и требований к тестированию (испытаниям).

Архитектура компонентов ПО ТПС должна соответствовать предъявляемым к ним в техническом задании требованиям (в том числе УПБ ПО ТПС), а также принятым методам проектирования.

6.9 При кодировании осуществляют написание исходного кода программы с применением выбранного языка программирования и по заданному алгоритму. Данный вид работы документируют в виде файловой структуры текста программы, в которой по согласованию с заказчиком приводят ссылку на носитель информации с исходным текстом программы по ГОСТ 19.401 или в ином формате, удовлетворяющем требования заказчика.

6.10 Интеграция ПО ТПС предусматривает сборку разработанных модулей и встроенного программного обеспечения реального времени в соответствии с планом интеграции и тестирование агрегированных компонентов. Интеграция системы управления единицей ТПС заключается в сборке всех ее компонентов, включая ПО ТПС и оборудование.

При интеграции необходимо обеспечить интероперабельность, правильность и контролируемость программ в аппаратной среде.

6.11 Для обеспечения приемлемого уровня безошибочности ПО ТПС целесообразно при разработке ПО ТПС:

- применять методы нисходящего проектирования;

- обеспечивать модульность программ;

- осуществлять верификацию на каждой стадии жизненного цикла ПО ТПС;

- использовать проверенные модули и библиотеки модулей;

- разрабатывать документацию, которая пригодна для аудита;

- проводить аттестационные испытания.

Основные приемы, используемые при разработке ПО ТПС с заданным УПБ, и необходимость их применения приведены в [1].

6.12 После каждой стадии разработки ПО ТПС необходимо проводить верификацию, основными аспектами которой являются:

а) подтверждение выполнения ПО ТПС и его программных компонентов требований безопасности, установленных в технологической и эксплуатационной документации ПО ТПС с целью установления:

1) полноты и корректности реализации ПО ТПС функций управления и функций обеспечения безопасности движения поездов, установленных техническим заданием;

2) полноты соответствия требованиям киберзащищенности, установленных техническим заданием;

3) достаточности и обоснованности технических приемов и мероприятий, которые применены при разработке ПО ТПС;

4) полноты и корректности программ и методик испытаний;

5) полноты и корректности результатов испытаний ПО ТПС и системы управления ТПС в целом;

б) подтверждение выполнения ПО ТПС требований безопасности при проведении стендовых испытаний.

Основными целями верификации по аспекту, указанному в перечислении б), являются:

- подтверждение соответствия полученных характеристик ПО ТПС требуемым значениям;

- проверка корректности взаимодействия между собой частей программ и аппаратуры, интегрированных на данном этапе разработки;

- проверка работы ПО ТПС на стойкость к внешним воздействующим факторам.

Результаты верификации включают в документ "Доказательство безопасности" в качестве раздела отчета о мерах по управлению функциональной безопасностью и представляют в орган по сертификации или аккредитованную испытательную лабораторию (центр) при испытаниях ПО ТПС.

7 Требования к защищенности программного обеспечения

7.1 При разработке необходимо обеспечить защиту ПО ТПС от несанкционированного доступа к ПО ТПС, преднамеренного разрушения и хищения и несанкционированного копирования ПО или данных при:

- воздействиях человеческого фактора (хищение машинных носителей и документации ПО ТПС, нарушение работоспособности ПО ТПС и др.);

- подключении аппаратных средств для считывания программ и данных или их физического разрушения.

7.2 Передача информации из систем управления ТПС во внешние организации, кроме диспетчерских и ситуационных центров, владельцев инфраструктуры или железнодорожных администраций государств, применяющих настоящий стандарт, не допускается.

Передача информации в диспетчерские и ситуационные центры должна идти только по закрытым каналам связи в зашифрованном виде.

При необходимости получения технической информации разработчиком, а также организацией, осуществляющей сервисное обслуживание ТПС в период опытной и постоянной эксплуатации, состав информации и процедура ее передачи должны быть согласованы с заказчиком при разработке технического задания и заключении договора на разработку или сервисное обслуживание единицы ТПС.

7.3 Защита от несанкционированного доступа к ПО ТПС и данным может быть обеспечена следующими способами:

- идентификацией и аутентификацией субъектов доступа и объектов доступа;

- управлением правами и привилегиями субъектов доступа, разграничением доступа субъектов доступа к объектам доступа на основе совокупности установленных в системе управления единицей ТПС правил разграничения доступа;

- ограничением программной среды;

- защитой машинных носителей информации;

- регистрацией событий безопасности;

- антивирусной защитой, в том числе обнаружением в системе управления единицей ТПС компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации;

- контролем (анализом) защищенности информации;

- обеспечением целостности программной среды и информации;

- применением правовых методов защиты ПО ТПС и др.

Применение тех или иных способов защиты и конкретные требования к ним устанавливаются положениями национального законодательства, национальными стандартами и нормативными документами, действующими на территории государств, применяющих настоящий стандарт.

7.4 Правовые методы защиты ПО ТПС должны быть установлены в лицензионных соглашениях и договорах, в которых оговариваются все условия эксплуатации программ, в том числе создание копий и хранение исходных тестов программ.

8 Требования к поставке и хранению программного обеспечения

8.1 ПО поставляют заказчику после проведения интеграционных испытаний программно-аппаратных средств на единице ТПС согласно ГОСТ 15.902.

8.2 Комплект поставки ПО ТПС заказчику оговаривается в договоре.

8.3 Установка ПО ТПС должна производиться с эталонного носителя.

8.4 Исходный и исполняемый коды ПО ТПС на электронных носителях информации, а также необходимые эксплуатационные документы, программные и иные инструменты разработки должны храниться в месте, исключающем возможность несанкционированного доступа к ним лиц, не имеющих на то полномочий. Место хранения и доступ к указанным материалам должны быть определены в договоре.

Электронные носители информации с ПО ТПС должны храниться в подразделениях заказчика, эксплуатирующих соответствующие программно-аппаратные комплексы, в условиях, исключающих несанкционированный доступ к ним. Если для доступа к программам имеются пароли, то они должны быть предоставлены заказчику.

Допускается хранение эталонных носителей информации, содержащих исходные тексты ПО ТПС, в арендованных банковских ячейках при условии, что к ним возможен только совместный доступ представителей эксплуатирующей организации и разработчика.

8.5 После поставки не допускается одностороннее изменение разработчиком защитных паролей, ограничения доступа, функций ПО ТПС, влияющее на работоспособность, диагностирование и эксплуатацию ТПС. Внесение изменений в ПО ТПС осуществляют согласно процедуре сопровождения и модификации, приведенной в разделе 9.

9 Требования к процедуре сопровождения и модификации программного обеспечения

9.1 Целью сопровождения и модификации является выявление и устранение обнаруженных дефектов и ошибок в программах и данных, введение новых функций и компонентов в ПО ТПС, анализ состояния и корректировка документации, тиражирование и контроль распространения версий ПО ТПС, актуализация и обеспечение сохранности документации и физических носителей.

Общий порядок проведения экспертизы модификации ПО ТПС определен в [1].

9.2 Все вносимые изменения в ПО ТПС могут быть приняты, только после оценки ПО ТПС и выдачи экспертного заключения испытательной лаборатории (центра), аккредитованной(ого) в установленном порядке на право проведения работ по испытаниям ПО ТПС.

9.3 Заявка на изменение декларированного ПО ТПС может быть подана разработчиком, изготовителем или заказчиком при наличии следующих причин:

- безопасность в процессе эксплуатации, по мнению заявителя, ниже необходимой или заданной;

- выявления скрытых ошибок ПО ТПС;

- ошибки в требованиях к функциональным характеристикам ПО ТПС, выявленные в процессе эксплуатации;

- модификация комплекса технических средств, замена элементной базы или модификация использования комплекса технических средств;

- изменение требований безопасности.

9.4 Подробности модификации и причин, повлекших внесение изменений, должны быть изложены в документации, в которой должны быть ссылки на:

- заявку на изменение;

- результаты экспертизы влияния предложенной модификации ПО ТПС на безопасность и принятые решения;

- отклонения от нормальной эксплуатации и нормальных условий;

- всю содержащуюся в документации информацию, на которую повлияла модификация.

9.5 Независимый эксперт, проводящий оценивание влияния предложенных изменений, должен идентифицировать:

- элементы конфигурации ПО ТПС и соответствующее базовое состояние, на которые влияет предложенное изменение;

- любые утвержденные модификации, влияющие на идентифицированные элементы конфигурации ПО ТПС.

Эксперт, проводящий оценивание влияния предложенных изменений, должен оценить,

насколько предложенное изменение является критичным, как оно влияет на безопасность.

Эксперт должен выявить, обосновать и записать значимость влияния предложенных изменений и предложений по усовершенствованию на продолжительность испытаний модифицированного ПО ТПС.

9.6 Повторные испытания в целях оценки соответствия проводят в том случае, если вносимые изменения повлияли на структуру ПО ТПС и могут быть критичными для безопасности и иметь технические риски.

9.7 Разработчик ПО ТПС должен записать последовательность работ и задач для реализации каждой утвержденной модификации и обеспечить, чтобы в базовые состояния включались только утвержденные изменения.

9.8 Целесообразно, чтобы изменения в документации к ПО ТПС анализировали эксперты испытательной лаборатории (центра), в котором ранее проводили испытания и экспертиза документации к данному ПО ТПС. Допускается проводить анализ изменений документации в других испытательных лабораториях (центрах), аккредитованных в установленном порядке, в случае отсутствия возможности провести данный анализ в испытательной лаборатории (центре), в котором ранее проводились испытания и экспертиза документации к данному ПО ТПС.

9.9 Характер изменений ПО ТПС должен обязательно быть отражен в программной документации на всех уровнях, включая рабочую (проектную) и эксплуатационную документацию. Документы должны быть повторно согласованы и утверждены после включения соответствующих изменений.

9.10 Разработчик должен поддерживать принятое экспертами и уполномоченными по изменению решение по утверждению, отклонению или отсрочке для каждого предложенного изменения, извещая о принятом решении тех лиц, кого оно касается.

9.11 Если решение отсрочено, разработчику следует представить рекомендации, как действовать до повторного рассмотрения.

9.12 Если изменение отклонено, то разработчику следует информировать ответственных за инициацию внесения изменений, чтобы снять предложенное изменение с рассмотрения.

9.13 Процесс изменения ПО ТПС должен быть закончен формированием новой версии программного обеспечения. Утвержденное изменение записывают на электронный носитель информации, идентифицируют надлежащим образом с помощью контрольной суммы (с указанием метода ее получения) и в дальнейшем данный электронный носитель информации с изменениями используют как эталонный, с проставлением даты формирования носителя информации и приложением акта и протокола идентификации версии ПО ТПС.

9.14 Для сведения риска повреждения программно-аппаратных комплексов и встроенных систем к минимуму, необходим жесткий контроль внесения изменений в них. Для этого требуются формальные процедуры управления процессом внесения изменений. Эти процедуры должны гарантировать, что функциональная безопасность и процедуры управления ею не будут нарушены и что получено формальное разрешение на внесение изменений.

9.15 Рекомендуется присваивать предложению об изменении уникальный идентификационный номер на самой ранней стадии, чтобы облегчить прослеживаемость и идентификацию. Следует фиксировать статус прохождения изменения и связанных с этим решений и распоряжений. Необходимо выполнять и документировать оценки предложенного изменения с точки зрения:

- его технических достоинств;

- влияния на взаимозаменяемость, средства сопряжения, а также необходимость повторной идентификации;

- влияния на график работы и расходы по договору;

- влияния на методы производства, испытания и контроля;

- влияния на закупки и запасы;

- влияния на техническое обслуживание, справочники для потребителя и руководства.

9.16 После подготовки изменения уполномоченное лицо или группа лиц должны проанализировать документированные оценки и решить вопрос об утверждении или неутверждении изменения. Внесение и проверка утвержденного изменения обычно включает следующие шаги:

- официальное утверждение изменения идентификации конфигурации;

- определение необходимых последующих действий соответствующими руководителями;

- проверка соответствия проекта, испытаний, производства и т.д. техническим требованиям.

9.17 Отчет пользователей о выявленных дефектах в программах должен содержать:

- идентификатор пользователя, представившего отчет;

- дату фиксирования дефекта или предложения на изменение ПО ТПС;

- номер и параметры адаптации версии ПО ТПС, на которой обнаружен дефект;

- подробное описание сценария и исходных данных, при которых выявлен дефект;

- описание проявления дефекта и документы результатов его регистрации;

- предположение о причине, вызвавшей проявление дефекта.

Отчет о предложениях по совершенствованию и развитию функций версии ПО ТПС, а также результатов анализа предполагаемых корректировок должен содержать:

- идентификатор разработчика, которому передан отчет пользователя для анализа предложения;

- дату анализа отчета пользователя;

- признак наличия повторяемости результатов и сценария проявления дефекта и информацию о необходимости дальнейшего анализа дефекта;

- тесты, исходные данные и сценарий, при которых проявляется дефект;

- результаты анализа предложения на изменение, причины и источника выявленного дефекта;

- рекомендации о возможных способах устранения дефекта или о реализации предложения по совершенствованию ПО ТПС;

- предложение по модификации ПО ТПС и его компонентов для устранения дефекта или совершенствования функционирования программ;

- оценки сложности, трудоемкости, эффективности и срочности модификации программ и базы данных;

- оценки влияния предлагаемых изменений на эксплуатацию версий ПО ТПС, имеющихся у пользователей.

9.18 Отчет о подготовленных и утвержденных корректировках, а также реализованных изменениях и обобщенных характеристиках новой версии программного обеспечения должен содержать:

- идентификатор специалиста, который разработал модификацию ПО ТПС;

- дату разработки модификации;

- причину изменения ПО ТПС (дефект, совершенствование);

- содержание изменений ПО ТПС;

- содержание изменений документации на версию программного обеспечения;

- результаты тестирования новой версии программного обеспечения с разработанными изменениями;

- дату и ответственное лицо, утвердившее модификацию ПО ТПС;

- содержание решения на изменения: частная модификация или издание новой версии программного обеспечения;

- результаты испытаний, обобщенные характеристики и идентификацию новой версии программного обеспечения после внесения изменений;

- решение по распространению пользователям новой версии программного обеспечения;

- решение по продолжению поддержки сопровождения предшествующих версий программного обеспечения;

- адрес хранения корректировок, документов и квалификационных тестов новой версии ПО ТПС.

9.19 Отчет о результатах эксплуатации снятой с сопровождения версии ПО ТПС и ее архивации должен содержать:

- дату решения о прекращении сопровождения определенной версии ПО ТПС и извещения пользователей;

- идентификатор ответственного лица, принявшего решение о прекращении сопровождения версии ПО ТПС;

- дату и идентификатор лица, выполнившего архивацию версии ПО ТПС;

- идентификаторы электронных носителей архива, содержащих подлинники и дубликаты текстов и документов, снятой с сопровождения версии ПО ТПС.

9.20 Журнал тиражирования версий, их характеристик, учета конфигураций и параметров версий ПО ТПС должен содержать:

- идентификаторы версий ПО ТПС, поддерживаемых сопровождением;

- краткую характеристику версий ПО ТПС;

- адрес архива, содержащего электронные носители и документацию каждой версии ПО ТПС;

- краткую характеристику и адрес архива, содержащего квалификационные тесты версий ПО ТПС;

- перечень идентификаторов пользователей, которым передана на эксплуатацию версия ПО ТПС;

- номер версии ПО ТПС, которая адаптировалась для эксплуатации каждым пользователем;

- параметры среды пользователя, на которые адаптировалась версия ПО ТПС;

- характеристики обращений пользователя к поставщику за консультациями и модификациями.

9.21 При внесении изменений следует проводить анализ ПО ТПС на предмет возможного

нарушения режима безопасности, проистекающий от таких изменений. Этот процесс должен включать в себя следующее:

- проверку процедур контроля приложений и обеспечения их целостности на предмет компрометации вследствие внесения изменений ПО ТПС;

- обеспечение своевременного уведомления испытательной лаборатории (центра) о предлагаемых изменениях в системе управления единицей ТПС для проведения надлежащего анализа до их внесения.

9.22 После получения протокола (экспертного заключения) испытаний проведенной модификации ПО ТПС разработчик должен оформить и зарегистрировать в органе по сертификации новую декларацию ПО ТПС, идентифицированного надлежащим образом с помощью контрольной суммы (с указанием метода ее получения).

Приложение А
(обязательное)

Набор показателей, обеспечивающих выполнение требований к качеству программного обеспечения

Таблица А.1 - Набор показателей, обеспечивающих выполнение требований к качеству программного обеспечения

Наименование показателя (характеристики)	Назначение и краткое описание показателя (характеристики)
1 Функциональная пригодность	Степень, с которой ПО ТПС предоставляет функции, которые отвечают заявленным и предполагаемым требованиям при использовании в заданных условиях
1.1 Функциональная полнота	Набор функций охватывает все указанные задачи и пользовательские задания
1.2 Функциональная корректность	ПО ТПС обеспечивает правильные результаты с необходимой степенью точности
1.3 Функциональная приспособляемость	Функции ПО ТПС облегчают достижение указанных целей и решение задач
2 Эффективность работы	Производительность по отношению к количеству используемых ресурсов при установленных условиях
2.1 Временной режим	Соответствие требованиям по времени реакции и обработки, производительности ПО ТПС при выполнении своих функций
2.2 Использование ресурсов	Соответствие требованиям количества и типов ресурсов, используемых ПО ТПС при выполнении своих функций
2.3 Потенциальные возможности	Максимальные пределы параметров ПО ТПС отвечают установленным требованиям
3 Совместимость	ПО ТПС осуществляет обмен информацией с другим ПО или его компонентами и/или выполняет требуемые функции, совместно используя ту же аппаратную или программную среду
3.1 Сосуществование	Эффективное выполнение требуемых функций, при совместном использовании общей среды и ресурсов с другим ПО ТПС, без вредного воздействия
3.2 Возможность взаимодействия	Использование информации, полученной ПО ТПС в результате обмена информацией с программными и аппаратными средствами разных поставщиков
4 Практичность	Использование ПО ТПС пользователем для достижения указанной цели эффективно, оперативно и адекватно в заданном контексте использования

4.1 Пригодность для распознаваемости	Определение степени, с которой пользователи могут распознать, является ли продукт или система подходящей для решения их задач
4.2 Обучаемость	Использование ПО ТПС пользователем для достижения заданной цели обучения эффективно, продуктивно, с отсутствием риска и с уверенностью удовлетворения в указанном контексте использования
4.3 Удобство и простота использования	Определение атрибутов, которые позволят легко эксплуатировать и управлять ПО ТПС или системой
4.4 Защита от ошибок пользователя	Определение степени защиты пользователя от совершения ошибок
4.5 Эстетика интерфейса пользователя	Интерфейс, обеспечивающий приятное и практичное взаимодействие пользователя с ПО ТПС
4.6 Доступность	Использование ПО ТПС людьми с различной степенью подготовки
5 Безотказность	Четкое выполнение ПО ТПС функций в определенных условиях в заданный период времени
5.1 Степень готовности ПО	Определение степени, с которой ПО ТПС отвечает требованиям безотказности при нормальной работе
5.2 Готовность	Определение степени нахождения ПО ТПС в рабочем состоянии и его доступности, когда это требуется для его использования
5.3 Отказоустойчивость	Правильное и четкое выполнение ПО ТПС основных функций, несмотря на наличие сбоев аппаратных средств или ПО ТПС
5.4 Способность к восстановлению	Возможность восстановления пострадавших данных и требуемого состояния ПО ТПС в случае прерывания обрыва или отказа
6 Защищенность	Установление степени защиты информации и данных от несанкционированного доступа
6.1 Конфиденциальность	Гарантии доступности информации и данных только для тех, кто уполномочен иметь доступ
6.2 Целостность	Предотвращение несанкционированного доступа с целью изменения компьютерных программ или данных
6.3 Отслеживаемость	Доказательство того, что действия или события имели место, чтобы невозможно было отказаться от авторства событий или действий
6.4 Подлинность	Установление степени подтверждения идентичности заявленного объекта или ресурса
7 Модифицируемость	Установление степени эффективности и продуктивности, с которой ПО ТПС может быть модифицировано при его сопровождении
7.1 Модульность	Характеристика ПО ТПС, определяющая такой состав дискретных компонентов, что изменение в одном из них оказывает минимальное воздействие на другие компоненты
7.2 Повторное использование	Используемость ПО ТПС в более чем одной системе или в создании других средств
7.3 Анализируемость	Степень эффективности и продуктивности, с которой можно оценить воздействие на ПО ТПС преднамеренного изменения одной или более частей, или провести диагностику продукта на предмет недостатков или причин отказов, или идентифицировать компоненты, которые должны быть изменены
7.4 Модернизируемость	Возможность изменения без привнесения дефектов или ухудшения существующего качества ПО ТПС
7.5 Контролируемость	Установление критериев испытаний ПО ТПС или его компонентов, которые позволят при проведении испытаний определить их выполнение
8 Переносимость	Возможность перенесения аппаратно-программного обеспечения в другую эксплуатационную среду
8.1 Адаптируемость	Адаптирование (приспособление) ПО ТПС для различного или вновь появляющегося оборудования, ПО ТПС или других эксплуатационных и используемых сред

8.2 Устанавливаемость	Степень эффективности и продуктивности, с которой ПО ТПС может быть успешно установлено и/или удалено в указанной среде
8.3 Заменяемость	Возможность использования другого ПО ТПС для той же цели в той же окружающей среде

Применение приведенных в таблице А.1 показателей качества - по [5].

Библиография

[1] МЭК 61508-3:2010 (IEC 61508-3:2010) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению (Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements)

[2] ЕН 50128:2011 (EN 50128:2011) Применение для железнодорожного транспорта - Системы связи, сигнализации и обработки данных - Программное обеспечение для железнодорожных систем управления и защиты (Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems)

[3] ИСО/МЭК 16085:2006[1)] (ISO/IEC 16085:2006) Системная и программная инженерия - Процессы жизненного цикла - Менеджмент риска (Systems and software engineering - Life cycle processes - Risk management)

[4] ИСО/МЭК 27005:2011[2)] (ISO/IEC 27005:2011) Информационная технология - Методы и средства обеспечения безопасности - Менеджмент риска информационной безопасности (Information technology - Security techniques - Information security risk management)

[5] ИСО/МЭК 25010:2011[3)] (ISO/IEC 25010:2011) Проектирование систем и разработка программного обеспечения. Требования к качеству систем и программного обеспечения и их оценка (SQuaRE). Модели качества систем и программного обеспечения (Systems and software engineering. Systems and software quality requirements and evaluation (SQuaRE). System and software quality models)

[1)] В Российской Федерации действует ГОСТ Р ИСО/МЭК 16085-2007 "Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения".

[2)] В Российской Федерации действует ГОСТ Р ИСО/МЭК 27005-2010 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности".

[3)] В Российской Федерации действует ГОСТ Р ИСО/МЭК 25010-2015 "Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов".

УДК 629.4.018:006.354 МКС 35.080
45.060

Ключевые слова: программное обеспечение, система управления, тяговый подвижной состав, требование

подготовлен АО "Кодекс" и сверен по:
официальное издание
М.: Стандартинформ, 2017