МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)

INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 33896— 2016

СИСТЕМЫ ДИСПЕТЧЕРСКОЙ ЦЕНТРАЛИЗАЦИИ И ДИСПЕТЧЕРСКОГО КОНТРОЛЯ ДВИЖЕНИЯ ПОЕЗДОВ

Требования безопасности и методы контроля

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

Цели, основные принципы и общие правила проведения работ по межгосударственной стандартизации установлены ГОСТ 1.0 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» («ВНИИНМАШ»), Федеральным государственным образовательным учреждением высшего профессионального образования «Петербургский государственный университет путей сообщения» (ФГОУ ВПО ПГУПС) и Акционерным обществом «Научно-исследовательский институт железнодорожного транспорта» (АО «ВНИИЖТ»)

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. № 93-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	Минэкономики Республики Армения
Грузия	GE	Грузстандарт
Казахстан	KZ	Госстандарт Республики Казахстан
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Таджикистан	TJ	Таджикстандарт
Узбекистан	UZ	Узстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 31 марта 2017 г. № 235-ст межгосударственный стандарт ГОСТ 33896—2016 введен в действие в качестве национального стандарта Российской Федерации с 1 ноября 2017 г.

5 Стандарт подготовлен на основе применения ГОСТ Р 54899—2012[1)]

6 ВВЕДЕН ВПЕРВЫЕ

7 ПЕРЕИЗДАНИЕ. Сентябрь 2019 г.

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация будет опубликована на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

[1)] Приказом Федерального агентства по техническому регулированию и метрологии от 31 марта 2017 г. № 235-ст ГОСТ Р 54899–2012 отменен с 1 ноября 2017 г.

© Стандартинформ, оформление, 2017, 2019

В Российской Федерации настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Требования безопасности 3
4.1 Функции, реализуемые системами диспетчерской централизации и диспетчерского контроля . . 3
4.2 Требования к реализации функций телесигнализации в системах диспетчерской централизации и диспетчерского контроля 4
4.3 Требования к реализации функций телеуправления диспетчерской централизации 5
4.4 Ответственные команды телеуправления диспетчерской централизации 5
4.5 Требования к эксплуатационной совместимости диспетчерской централизации и диспетчерского контроля 6
4.6 Требования к аппаратным и программным средствам диспетчерской централизации и диспетчерского контроля 7
4.7 Критерии опасных отказов диспетчерской централизации и диспетчерского контроля 7
5 Методы контроля 8
5.1 Общие положения 8
5.2 Контроль требований безопасности к функциям, реализуемым диспетчерской централизацией и диспетчерским контролем 10
5.3 Контроль требований безопасности к эксплуатационной совместимости диспетчерской централизации и диспетчерского контроля 10
5.4 Контроль требований безопасности к аппаратным и программным средствам диспетчерской централизации и диспетчерского контроля 11

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

СИСТЕМЫ ДИСПЕТЧЕРСКОЙ ЦЕНТРАЛИЗАЦИИ И ДИСПЕТЧЕРСКОГО КОНТРОЛЯ ДВИЖЕНИЯ ПОЕЗДОВ

Требования безопасности и методы контроля

Centralized traffic and dispatching control systems of trains movement.
Safety requirements and methods of checking

Дата введения — 2017—11—01

1 Область применения

Настоящий стандарт распространяется на системы диспетчерской централизации и диспетчерского контроля движения поездов.

Настоящий стандарт устанавливает функции и условия безопасного функционирования систем диспетчерской централизации и диспетчерского контроля движения поездов, значения параметров, обеспечивающих их безопасность, критерии опасных отказов, а также требования к аппаратно-программным средствам диспетчерской централизации и диспетчерского контроля.

Настоящий стандарт применяют при разработке, проектировании и изготовлении аппаратных и программных средств диспетчерской централизации и диспетчерского контроля движения поездов и оценке соответствия вновь разрабатываемых и импортируемых систем диспетчерской централизации и диспетчерского контроля требованиям безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие межгосударственные стандарты:

ГОСТ 26.005 Телемеханика. Термины и определения

ГОСТ 9238 Габариты железнодорожного подвижного состава и приближения строений

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

ГОСТ 33436.4-1 Совместимость технических средств электромагнитная. Системы и оборудование железнодорожного транспорта. Часть 4-1. Устройства и аппаратура железнодорожной автоматики и телемеханики. Требования и методы испытаний

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации (gost.e-ecolog.ru по указателям национальных стандартов, издаваемым в государствах, указанных в предисловии, или на официальных сайтах соответствующих национальных органов по стандартизации. Если на документ дана недатированная ссылка, то следует использовать документ, действующий на текущий момент, с учетом всех внесенных в него изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то следует использовать указанную версию этого документа. Если после принятия настоящего стандарта в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение применяется без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ 26.005, а также следующие термины с соответствующими определениями:

3.1 **железнодорожная автоматика и телемеханика;** ЖАТ**:** Подсистема инфраструктуры железнодорожного транспорта, включающая в себя комплекс технических сооружений и устройств сигнализации, централизации и блокировки, обеспечивающих управление движением поездов на перегонах и станциях и маневровой работой.

Примечание — Железнодорожная автоматика и телемеханика — это также область науки и техники, связанная с ее разработкой, производством и технической эксплуатацией.

3.2 **диспетчерская централизация** (железнодорожный транспорт); ДЦ: Система телемеханического централизованного управления и контроля объектами диспетчерского участка на основе объединения устройств железнодорожной автоматики и телемеханики железнодорожных станций и перегонов.

3.3 **диспетчерский контроль** (железнодорожный транспорт); ДК: Система телеконтроля состояний и телеизмерений параметров объектов железнодорожной автоматики и телемеханики на железнодорожных станциях и перегонах диспетчерского участка.

3.4 **условия безопасности движения железнодорожных поездов:** Совокупность контролируемых состояний путевых объектов, железнодорожного подвижного состава, смежных систем и устройств, при которых обеспечивается безопасное движение железнодорожных поездов.

3.5 **критерий опасного отказа железнодорожной автоматики и телемеханики:** Признак или совокупность признаков опасного состояния системы железнодорожной автоматики и телемеханики, установленные в нормативных документах и (или) конструкторской документации.

3.6 **комбинированное управление станцией:** Режим управления железнодорожной станцией на участке диспетчерской централизации, при котором поездной диспетчер управляет движением железнодорожных поездов по главным и боковым путям для безостановочного пропуска поездов, а по остальным железнодорожным путям, изолированным охранным положением стрелок, управление движением осуществляет дежурный по железнодорожной станции (маневровый диспетчер).

3.7 **полигон диспетчерского управления:** Зона управления перевозочным процессом, интегрированная в диспетчерском центре по технологическим соображениям.

3.8 **электрическая централизация стрелок и светофоров:** Станционная система централизованного управления и контроля за объектами железнодорожной автоматики и телемеханики с обеспечением установленных требований безопасности движения железнодорожных поездов и заданной пропускной способности.

Примечание — Различают электрическую централизацию стрелок и светофоров:

- релейная централизация, где все функции управления и контроля за объектами железнодорожной автоматики и телемеханики станции реализуются с помощью релейных устройств;
- релейно-процессорная централизация, где функции маршрутного управления реализуются программно-аппаратными средствами, функции обеспечения зависимостей между стрелками, светофорами и маршрутами, а также функции управления и контроля за напольными объектами реализуются с помощью релейных устройств;
- микропроцессорная централизация, где функции маршрутного управления, функции обеспечения зависимостей между стрелками, светофорами и маршрутами реализуются программно-аппаратными средствами, а функции управления и контроля за напольными объектами могут реализовываться с помощью программно-аппаратных или релейных устройств.

3.9 **ответственная команда** (железнодорожная автоматика и телемеханика): Команда, передаваемая с пульта управления диспетчерской или электрической централизации стрелок и светофоров, выполняемая под ответственность дежурного персонала по управлению движением железнодорожных поездов с исключением проверки устройствами железнодорожной автоматики и телемеханики отдельных условий безопасности.

3.10 **станция автономного управления:** Железнодорожная станция на участке диспетчерской централизации, управление которой осуществляет дежурный по станции под контролем поездного диспетчера.

3.11 **станция диспетчерского управления:** Железнодорожная станция на участке диспетчерской централизации, управление которой в нормальном режиме осуществляет поездной диспетчер.

3.12 **станционное управление на участке диспетчерской централизации:** Режим работы станции диспетчерского управления, при котором она находится под управлением дежурного по станции.

3.13 **местное управление объектами железнодорожной станции:** Управление объектами района железнодорожной станции с маневровой колонки или маневрового поста.

3.14 **резервное управление на участке диспетчерской централизации:** Режим управления железнодорожной станцией участка диспетчерской централизации с местного аппарата управления системы электрической централизации при отсутствии возможности осуществления диспетчерского управления.

4 Требования безопасности

4.1 Функции, реализуемые системами диспетчерской централизации и диспетчерского контроля

4.1.1 Системы ДЦ и ДК должны обеспечивать выполнение следующих функций телесигнализации:

а) сбор и отображение для поездного диспетчера в реальном времени данных о состоянии всех объектов, контролируемых системами электрической централизации стрелок и светофоров (ЭЦ) и автоматической блокировкой (АБ) участка железнодорожной линии;

б) автоматизированная передача информации операторам вышестоящего и смежного уровней управления движением железнодорожных поездов (далее — поезда) с обеспечением требований информационной безопасности;

в) фиксация и выдача актуальной информации по нахождению железнодорожного подвижного состава (подвижного состава) на объектах путевого развития;

г) информационное взаимодействие с локомотивными устройствами безопасности по радиоканалу (при установке необходимого оборудования связи на диспетчерском участке и локомотивах);

д) автоматическое ведение графика исполненного движения поездов и приложения к нему;

е) расчет ожидаемого времени проследования поездов по станциям участка железнодорожной линии;

ж) выявление возможных конфликтных ситуаций в организации движения поездов;

и) расчет и корректировка прогнозного графика движения поездов;

к) формирование диспетчерских приказов и предупреждений;

л) ведение диспетчерского журнала;

м) протоколирование эксплуатационных событий с возможностью воспроизведения архивированных данных;

н) логический анализ эксплуатационных событий и действий персонала;

п) мониторинг состояния технических средств ДЦ и передача информации в систему диагностики и мониторинга ЖАТ железнодорожного участка;

р) автоматизированный учет показателей движения поездов и производимых работ;

с) контроль выполнения технологических этапов перевозочного процесса на участке железнодорожной линии;

т) слежение за перемещениями подвижных средств и организация динамических моделей поездного, локомотивного, вагонного положений на участке железнодорожной линии;

у) формирование и выдача сведений о поезде:

1) номер поезда,
2) местоположение,
3) длина состава,
4) вес поезда,
5) натурные листы,
6) разложение по дорогам назначения и плану формирования,
7) история поезда;

ф) формирование и выдача сведений о локомотиве:

1) серия и номер,
2) депо приписки,
3) фактическое местоположение,
4) история,
5) учет времени по прибытию и отправлению,
6) расчет простоя,
7) подвязка бригад локомотивов к ниткам графика движения поездов,

8) плановые сроки обслуживания и ремонта;

х) формирование и выдача сведений о вагонах:

1) идентификационный номер,

2) местоположение,

3) состояние,

4) вагонный лист;

ц) формирование нормативно-справочной информации и запросов в смежные системы;

ч) продвижение по участку номера поезда после ввода в систему с пульта поездного диспетчера, со средств идентификации или трансляции со смежного участка;

ш) фиксация изменений в состоянии контролируемых объектов и формирование соответствующих сообщений;

щ) контроль единого времени и актуальности используемой информации.

4.1.2 Системы ДЦ должны обеспечивать выполнение следующих функций телеуправления:

- диспетчерское управление поездной работой на участках, линиях, направлениях;
- диспетчерское управление движением высокоскоростных поездов на участках железнодорожных линий со смешанным движением поездов;
- диспетчерское управление маневровой работой на железнодорожных станциях (станциях) диспетчерского участка;
- передача управления станцией диспетчерского участка на станционное управление дежурным по станции при исправных средствах телемеханики;
- передача группы объектов ЭЦ станции диспетчерского управления на местное управление составителю поездов;
- перевод станции на комбинированное управление, когда на станции автономного управления главные пути и пути безостановочного пропуска передаются в управление поездного диспетчера;
- изменение режимов управления станцией, районом, объектом участка (режимы управления: диспетчерское, станционное, местное) с сохранением единоначалия в любой момент времени;
- изменение границ зоны управления с рабочего места (поездного диспетчера, дежурного по станции, оператора местного управления) с соблюдением принципа единоначалия;
- формирование команд управления объектами ЭЦ, АБ и полуавтоматической блокировкой (ПАБ) в разных эксплуатационных режимах (индивидуальное управление объектами, маршрутное управление, автоматическое управление по накопленной программе);
- передача и контроль реализации команд управления объектами ЭЦ, АБ и ПАБ;
- формирование ответственных команд телеуправления (по утвержденному заказчиком перечню) с обеспечением их безопасной передачи системам ЭЦ, АБ и ПАБ;
- автоматическое двукратное реверсирование стрелочного электропривода и возвращение остряков централизованной стрелки в исходное состояние в случае отсутствия контроля требуемого положения этой стрелки в заданное время;
- формирование команды экстренной остановки движения локомотива;
- формирование команд управления заградительными сигналами.

4.2 Требования к реализации функций телесигнализации в системах диспетчерской централизации и диспетчерского контроля

Для организации безопасного движения поездов аппаратура каналов телесигнализации (ТС) в системах ДЦ и ДК должна обеспечивать:

- отображение для поездного диспетчера в реальном времени (не нарушая хронологии событий и с задержкой по времени не более 6 с) данных о состоянии всех объектов, контролируемых системами ЭЦ, АБ и ПАБ участка железнодорожной линии;
- автоматическое преобразование исходной информации в нужную форму при передаче сообщений операторам вышестоящего и смежного уровней системы управления перевозочным процессом;
- исключение использования поездным диспетчером неактуальной информации для управления движением в случае задержки передачи сообщений по каналу ТС более чем на 1 мин;
- протоколирование эксплуатационных событий с возможностью воспроизведения архивированных данных в течение не менее 10 сут;
- контроль непрерывности связи по каналу ТС с требуемой достоверностью приема сообщений;
- гальваническую развязку входных цепей устройств сопряжения с контролируемыми устройствами ЖАТ;

- вероятность трансформации сигнала ТС более 10^{-8};
- вероятность потери информации в канале ТС не более 10^{-8};
- вероятность ложного контрольного сообщения при отсутствии передачи не более 10^{-12};
- время готовности системы ДЦ и ДК к работе при включении питания не более 3 мин.

4.3 Требования к реализации функций телеуправления диспетчерской централизации

В системах ДЦ при организации телеуправления (ТУ) объектами ЖАТ необходимо в целях обеспечения безопасности движения поездов обеспечивать:

а) разграничение и изменение зон управления между операторами таким образом, чтобы в любой момент правом управления тем или иным объектом обладал только один оператор (соблюдение принципа единоначалия);

б) передачу возможности управления тем или иным объектом другому оператору по установленной процедуре с регистрацией согласованных действий операторов;

в) перевод железнодорожной станции со станционного управления на диспетчерское должен происходить при выполнении следующих условий:

1) наличие в замках аппаратов управления ключей-жезлов,
2) отсутствие начавшейся реализации ответственных команд,
3) отсутствие блокированных объектов,
4) отсутствие централизованных стрелок, выключенных из зависимостей,
5) отсутствие индивидуального замыкания стрелок и/или путевых участков,
6) отсутствие искусственного размыкания путевых участков,
7) отсутствие закрытия переезда управляющей директивой,
8) отсутствие незаконченных действий, начатых в режиме станционного управления,
9) отсутствие передачи управления стрелками и светофорами на местное управление;

г) исключение использования устаревшей информации о состоянии объектов для формирования управляющих команд;

д) использование режима накопления маршрутов и программного управления только для станций участка, оборудованных устройствами ЭЦ с защитой от преждевременного размыкания централизованной стрелки при кратковременном нарушении шунтирования рельсовой цепи стрелочной секции маршрута;

е) время реакции системы ДЦ на управляющее воздействие оператора автоматизированного рабочего места — не более 500 мс;

ж) время от момента ввода команды до начала ее реализации объектом управления — не более 1 с;

и) время хранения на контролируемом пункте предварительной части ответственной команды в ожидании исполнительной части команды управления объектом — не более 30 с;

к) длительность формирования серии посылок исполнительной части ответственной команды управления объектом (при спорадической передаче сигналов ТУ) — не более 3 мин с интервалом между посылками серий не более 15 с;

л) исключение формирования других команд ТУ во время посылки ответственной команды;

м) вероятность трансформации сигнала ТУ — не более 10^{-14};

н) вероятность потери информации в канале ТУ — не более 10^{-10};

п) вероятность генерации ложной команды ТУ при отсутствии передачи — 10^{-12};

р) интенсивность опасных отказов технических средств передачи и реализации ответственных команд — не более $3 \cdot 10^{-11}$ 1/ч на одну команду.

4.4 Ответственные команды телеуправления диспетчерской централизации

4.4.1 Для обеспечения непрерывности перевозочного процесса при возникновении некоторых неисправностей в устройствах ЖАТ должен использоваться вспомогательный режим управления объектами путем передачи ответственных команд ТУ. Ответственная команда ТУ предполагает управляющее воздействие на объект ЖАТ с исключением схемной проверки отдельных блокировочных зависимостей, обеспечивающих безопасность движения поездов.

Использование вспомогательного режима допустимо только после проверки на месте работником службы перевозок или другим уполномоченным лицом фактического состояния соответствующего неисправного объекта ЖАТ (железнодорожного стрелочного перевода, изолированного участка, станционных железнодорожных путей, железнодорожного перегона, переезда, поезда и т. д.). Передача ТУ во вспомогательном режиме должна быть санкционирована ответственным лицом, назначенным

руководителем единой диспетчерской смены дорожного центра управления перевозками. При этом ответственное лицо должно убедиться, что поездной диспетчер располагает достаточной информацией для безопасного применения вспомогательного режима.

4.4.2 Автоматизированная система диспетчерского управления движением поездов должна обеспечивать возможность передачи на контролируемые пункты станций зоны диспетчерского управления следующих ответственных команд:

- вспомогательная смена направления движения по пути перегона, оборудованного двухсторонней автоматической блокировкой (или автоматической блокировкой в одном направлении и автоматической локомотивной сигнализацией в другом), при ложной занятости рельсовых цепей (или других устройств контроля) пути перегона;
- вспомогательный режим подачи сигнала прибытия железнодорожного поезда в полном составе на железнодорожную станцию на участках железнодорожных линий, оборудованных полуавтоматической блокировкой с устройством автоматического контроля свободности перегона, при ложно занятом состоянии пути перегона;
- вспомогательный перевод железнодорожных стрелок при ложно занятом состоянии изолированного участка железнодорожного пути;
- отмена замыкания железнодорожных стрелок, замкнутых командой ТУ поездного диспетчера «Искусственное замыкание»;
- искусственное размыкание замкнутых в маршруте изолированных участков пути, не разомкнувшихся автоматически после использования маршрута;
- выключение извещения на переезд, расположенный в пределах железнодорожной станции, поданного командой ТУ поездного диспетчера «Закрытие переезда»;
- вспомогательное отключение устройства контроля схода подвижного состава из схемы включения разрешающего сигнального показания входного светофора при ложном срабатывании или неисправности устройства;
- вспомогательная отмена режима пропуска скоростного и высокоскоростного поезда, размыкание железнодорожных блок-участков, участков удаления, принудительной остановки локомотива и отмены принудительной остановки;
- вспомогательное отключение контрольно-габаритного устройства из схемы включения разрешающего сигнального показания выходного светофора при его ложном срабатывании или неисправности;
- снятие логической занятости изолированных участков пути;
- отмена блокирования пути перегона;
- отмена замыкания первого участка удаления.

4.5 Требования к эксплуатационной совместимости диспетчерской централизации и диспетчерского контроля

4.5.1 Конструкция аппаратных средств систем ДЦ и ДК, предназначенных для размещения около железнодорожных путей (напольное оборудование железнодорожной автоматики и телемеханики), должна отвечать требованиям габарита приближения строений ГОСТ 9238.

4.5.2 Технические средства систем ДЦ и ДК должны выполнять свои функции во всех предусмотренных при их разработке и (или) проектировании условиях и режимах, не создавая при этом препятствий для функционирования как других технических средств ЖАТ, так и остальных объектов инфраструктуры железнодорожной линии.

4.5.3 Параметры быстродействия систем ДЦ и ДК должны обеспечивать выполнение всех предусмотренных функций в заданном диапазоне скоростей и характеристик подвижных составов.

4.5.4 В соответствии с проектом по оборудованию участка железнодорожной линии технические средства систем ДЦ и ДК должны быть функционально, информационно и технически совместимыми с системами:

- ЖАТ на станциях;
- ЖАТ на перегонах железнодорожных линий;
- контроля технического состояния подвижного состава (средства автоматического контроля технического состояния подвижного состава на ходу поезда, устройство контроля схода подвижного состава, контрольно-габаритные устройства);
- идентификации и определения местоположения подвижного состава;
- контроля состояния устройств ограждения и закрепления железнодорожного подвижного состава, устройств переездной, мостовой, тоннельной, обвальной и других сигнализаций;

- информационными системами смежных и более высоких уровней управления перевозочным процессом.

4.5.5 Технические средства систем ДЦ и ДК должны обеспечивать безопасный интерфейс с другими системами ЖАТ, действующими на данном участке железнодорожной линии, или иметь возможность интегрировать функции этих систем.

4.5.6 Технические средства систем ДЦ и ДК должны разрабатываться с учетом выполнения требований электромагнитной совместимости в соответствии с ГОСТ 33436.4-1.

4.6 Требования к аппаратным и программным средствам диспетчерской централизации и диспетчерского контроля

4.6.1 Аппаратные и программные средства ДЦ и ДК должны быть разработаны, спроектированы и изготовлены таким образом, чтобы во всех режимах работы при соблюдении всех требований, установленных в эксплуатационной документации, обеспечивалась реализация всех функций по обеспечению безопасности движения поездов (см. 4.1) в течение установленного срока службы.

4.6.2 Одиночный отказ, допустимая последовательность отказов аппаратных средств ДЦ и ДК должны обнаруживаться с заданной вероятностью на рабочих и тестовых воздействиях не позднее чем в системе возникнет последующий отказ.

После обнаружения отказа, допустимой последовательности отказов средств передачи и реализации ответственных команд системы ДЦ данные средства должны переходить в необратимое защитное состояние.

4.6.3 Если концепцией построения программно-аппаратных средств ДЦ и ДК допускается накопление отказов, которые не обнаруживаются в процессе эксплуатации, то вероятность возникновения опасного отказа по причине их накопления за период эксплуатации не должна превышать заданной вероятности опасного отказа.

4.6.4 Программно-аппаратные средства ДЦ должны обеспечивать восстановление работоспособного состояния из необратимого защитного состояния только с участием эксплуатационного персонала.

4.6.5 Интенсивность опасных отказов технических средств передачи и реализации ответственных команд должна быть не более $3 \cdot 10^{-11}$ 1/ч на одну команду.

4.6.6 Программные средства, применяемые в ДЦ и ДК, как встраиваемые в аппаратные средства, так и поставляемые на носителях записи, должны:

- обеспечивать корректное выполнение всех функций по обеспечению безопасности движения поездов (см. 4.1);
- быть тестируемыми и диагностируемыми;
- сохранять работоспособность после перезагрузок, вызванных сбоями и отказами аппаратных средств и источников электропитания;
- контролировать целостность программ и данных;
- быть защищены от несанкционированного доступа, от потерь и искажений при хранении, вводе, выводе, возникновении сбоев при обработке информации;
- и не должны иметь свойств и характеристик, не описанных в технической документации на программные средства (недекларированные возможности).

4.7 Критерии опасных отказов диспетчерской централизации и диспетчерского контроля

4.7.1 Критериями опасного отказа систем ДЦ и ДК в процессе функционирования ТС являются следующие события:

- получение устаревших данных ТС после восстановления работоспособности контролируемого пункта или передачи по каналу передачи данных;
- сохранение устаревшей индикации на средствах отображения индикации у поездного диспетчера после прекращения поступления ТС;
- неправильная индикация состояния контролируемых объектов у поездного диспетчера при пользовании ответственными командами или при организации движения поездов по приказам.

4.7.2 Критериями опасного отказа систем ДЦ при выполнении функций ТУ являются:

- реализация на контролируемом пункте ответственной команды при отсутствии или передаче других команд;
- самопроизвольная (несанкционированная) генерация ответственной команды.

4.7.3 Критериями опасного отказа системы ДЦ при выполнении функции ТУ при разделении режимов управления между персоналом являются следующие события:

- возможность реализации команд ТУ (в т. ч. ответственных) от дежурного по железнодорожной станции и поездного диспетчера в случае, когда станция находится на комбинированном управлении, а также вследствие одновременного существования разных режимов управления станцией (диспетчерского и станционного, диспетчерского и резервного);

- возможность реализации команд ТУ (в т. ч. ответственных) от двух поездных диспетчеров при неправильном разграничении зон диспетчерского управления.

5 Методы контроля

5.1 Общие положения

5.1.1 Основными методами контроля систем ДЦ и ДК являются:

а) оценка соответствия системы ДЦ или ДК и ее составных частей требованиям безопасности в форме экспертизы проектной, конструкторской, технологической, программной, эксплуатационной документации.

Экспертная оценка на стадии разработки проводится с целью установления:

- полноты и корректности реализации системой функций по обеспечению безопасности движения поездов, установленных заданием на проектирование;

- достаточности и обоснованности технических приемов и мероприятий, которые применены в системе ДЦ или ДК, для реализации положений концепции обеспечения безопасности с целью исключения опасных отказов;

- полноты и корректности программ и методик испытаний;

- полноты и корректности результатов испытаний системы ДЦ или ДК и ее составных частей;

- обоснованности и корректности рассчитанных количественных показателей безопасности.

На стадии изготовления экспертиза проводится с целью оценки полноты и корректности выполнения требований разработчика при изготовлении системы ДЦ или ДК и ее составных частей.

Экспертиза на стадии эксплуатации проводится для оценки показателей безопасности функционирования системы в реальных условиях и режимах эксплуатации, технического обслуживания и ремонта;

б) оценка соответствия системы ДЦ или ДК и ее составных частей требованиям безопасности в форме испытаний.

На этапе разработки целью испытаний являются:

- подтверждение соответствия требованиям безопасности элементов системы ДЦ или ДК и программных компонент в форме автономных испытаний. По результатам этих испытаний определяется соответствие полученных характеристик этих элементов требуемым значениям, а также готовность перехода к этапу комплексных проверок;

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

- оценка эффективности системы защиты от сбоев и отказов аппаратных средств;

- проверка работы системы контроля и локализации отказов;

- возможность реконфигурации системы и обеспечения защитного состояния;

- проверка работы системы на стойкость к внешним воздействующим факторам, в том числе по требованиям электромагнитной совместимости в соответствии ГОСТ 33436.4-1;

- процедуры адаптации системы ДЦ или ДК к полигону внедрения выполнены корректно.

На этапе изготовления испытания проводятся с целью установления возможности обеспечения стабильного качества выпускаемой продукции.

Эксплуатационные испытания проводятся с целью подтверждения заявленных требований безопасности в реальных условиях и режимах эксплуатации, технического обслуживания и ремонта системы ДЦ или ДК;

в) расчетные методы обоснования количественных показателей безопасности системы ДЦ или ДК.

На этапе разработки расчетные методы используются для определения предполагаемого уровня безопасности программно-аппаратных средств системы ДЦ или ДК.

На этапе эксплуатации на основании статистических данных об отказах системы определяется фактический уровень безопасности системы ДЦ или ДК.

5.1.2 Методы контроля выполнения требований безопасности систем ДЦ и ДК должны быть согласованы с этапами разработки, изготовления и эксплуатации систем ДЦ и ДК.

Методы контроля приведены в таблице 1.

Перечень контролируемых требований на каждом этапе должен быть отражен в программе обеспечения безопасности. Результаты выполнения методов контроля должны быть представлены в документе «Доказательство безопасности».

Таблица 1

Стадия жизненного цикла	Номера подразделов, пунктов требований, подлежащих контролю	Метод контроля
Разработка	4.1, 4.5, 4.6.5	Экспертиза технического задания на систему в части функциональных требований и требований безопасности
	4.2—4.5	Экспертиза алгоритмического обеспечения системы
	4.6.2, 4.6.3	Экспертиза концепции обеспечения безопасности системы
	4.2—4.4	Экспертиза проектной оценки безопасности системы
	4.6	Экспертиза аппаратных и программных средств системы на соответствие положений концепции безопасности
	4.5, 4.6	Экспертиза технических решений
	4.1—4.4, 4.6.6	Испытания технологического программного обеспечения
	4.6.1—4.6.5	Испытания программно-аппаратных средств
	4.1—4.4	Экспертиза документа «Доказательство безопасности»
	4.5	Экспертиза эксплуатационной документации
	4.1—4.4, 4.5.4, 4.6.2, 4.6.4	Проведение автономных испытаний системы
Изготовление	4.2—4.4	Проведение приемочных испытаний системы
	В соответствии с программой и методикой испытаний	Проведение заводских испытаний системы
	4.1—4.6	Экспертиза проекта
Эксплуатация	4.2—4.5	Систематический сбор, обработка и анализ данных об отказах и сбоях, имевших место в процессе эксплуатации. Определение фактических значений количественных показателей безопасности и данных, накопленных в процессе эксплуатации, а также оценка соответствия этих показателей заданным значениям

5.1.3 Если в составе систем диспетчерской централизации или диспетчерского контроля применяются аппаратные и/или программные средства измерения, то

- все средства измерений должны быть утвержденного типа и поверены;
- применяемые методики измерений (кроме прямых измерений) должны быть аттестованы в соответствии с национальными стандартами и нормативными документами, действующими на территории государства, принявшего стандарт[1)];
- программное обеспечение, связанное с измерениями, должно быть аттестовано в соответствии с национальными стандартами и нормативными документами, действующими на территории государства, принявшего стандарт[2)].

[1)] В Российской Федерации действует ГОСТ Р 8.563—2009 «Государственная система обеспечения единства измерений. Методики (методы) измерений».

[2)] В Российской Федерации действуют:

- ГОСТ Р 8.654—2015 «Государственная система обеспечения единства измерений. Требования к программному обеспечению средств измерений. Основные положения»;
- МИ 2955—2010 «Рекомендация. Государственная система обеспечения единства измерений. Типовая методика аттестации программного обеспечения средств измерений».

5.2 Контроль требований безопасности к функциям, реализуемым диспетчерской централизацией и диспетчерским контролем

5.2.1 Контроль требований безопасности к функциям, реализуемым системами ДЦ и ДК, выполняется на основе проведения экспертизы проектной, конструкторской, технологической, программной, эксплуатационной документации, проверки наличия документации, подтверждающей выполнение проверяемых требований безопасности и испытаний.

5.2.2 На этапе разработки систем ДЦ и ДК организация-разработчик разрабатывает и согласовывает с организацией-заказчиком системы и испытательной лабораторией (центром), аккредитованной на проведение работ по оценке соответствия ЖАТ требованиям безопасности [испытательная лаборатория (центр)], документацию с описанием функций, реализуемых системой ЖАТ.

5.2.3 Испытательная лаборатория (центр) при участии организации-разработчика проводит экспертизу и испытания для подтверждения корректности реализации функций системами ДЦ и ДК.

5.2.4 При внесении изменений в программно-аппаратные средства систем ДЦ и ДК при добавлении функций, реализуемых этими системами, производятся повторное согласование документации, повторная экспертиза и испытания в испытательной лаборатории (центре).

5.2.5 При проектировании участка железнодорожной линии организация-проектировщик на основе проектной, конструкторской, технологической, программной, эксплуатационной документации должна определить необходимый набор функций, реализуемых системами ДЦ и ДК для данного полигона управления, и при необходимости согласовать с организацией-заказчиком системы и организацией-разработчиком требуемый объем доработок.

5.2.6 При вводе в эксплуатацию полнота и корректность функций, реализуемых системами ДЦ и ДК, должны быть подтверждены при проведении приемочных испытаний в объеме, предусмотренном программой и методикой приемочных испытаний. Программа и методика приемочных испытаний должны покрывать все функции, реализуемые системами ДЦ и ДК. Программа и методика испытаний должны разрабатываться организацией-разработчиком системы ДЦ или ДК и согласовываться с организацией-заказчиком системы и испытательной лабораторией (центром). В процессе эксплуатации системы ДЦ или ДК полнота и корректность реализуемых функций должны оцениваться по результатам мониторинга и статистических отчетов в соответствии с национальными стандартами и нормативными документами, действующими на территории государства, принявшего стандарт, по надежности в технике и сбору и обработке информации о надежности изделий в эксплуатации.

5.3 Контроль требований безопасности к эксплуатационной совместимости диспетчерской централизации и диспетчерского контроля

5.3.1 Контроль требований безопасности к эксплуатационной совместимости систем ДЦ и ДК выполняется на основе проведения экспертизы проектной, конструкторской, технологической, программной, эксплуатационной документации, проверки наличия документации, подтверждающей выполнение проверяемых требований безопасности и испытаний.

5.3.2 На этапе разработки систем ДЦ и ДК организация-разработчик разрабатывает и согласовывает с организацией-заказчиком документацию по увязке разрабатываемых систем ДЦ и ДК с другими системами ЖАТ, действующими на данном участке железнодорожной линии.

5.3.3 Испытательная лаборатория (центр) при участии организации-разработчика проводит экспертизу и испытания для подтверждения корректности реализации увязки разрабатываемой системы с другими системами ЖАТ.

5.3.4 При внесении изменений в технические решения по увязке систем ДЦ и ДК с другими системами производятся повторное согласование документации, повторная экспертиза и испытания в испытательной лаборатории (центре).

5.3.5 При проектировании железнодорожной линии в рамках экспертизы проекта проверяется выполнение требований к размещению аппаратных средств, функциональной, информационной, электромагнитной и конструктивной совместимости систем ДЦ и ДК.

5.3.6 Для этапа эксплуатации станционной системы ЖАТ корректность размещения аппаратных средств систем ДЦ и ДК, а также соответствие проекту должно быть подтверждено при проведении приемочных испытаний.

5.4 Контроль требований безопасности к аппаратным и программным средствам диспетчерской централизации и диспетчерского контроля

5.4.1 Контроль выполнения требований безопасности к аппаратным и программным средствам систем ДЦ и ДК должен выполняться на основе проведения экспертизы проектной, конструкторской, технологической, программной, эксплуатационной документации, подтверждающей выполнение проверяемых требований безопасности, расчетных методов и испытаний.

5.4.2 На этапе разработки системы ДЦ или ДК организация-разработчик должна разработать и согласовать с испытательной лабораторией (центром) документ «Доказательство безопасности» в соответствии с ГОСТ 33432. В документе «Доказательство безопасности» должно быть представлено аргументированное обоснование того, что программно-аппаратные средства системы ДЦ или ДК соответствуют предъявляемым к ним требованиям безопасности. Материалы документа «Доказательство безопасности» должны позволять сделать следующие выводы:

- требования на систему заданы корректно и в полном объеме;
- требования, предъявляемые к системе, в полном объеме и корректно реализованы в программно-аппаратных решениях;
- программно-аппаратные решения не привносят дополнительных негативных свойств относительно первоначальных требований безопасности;
- представленные доказательства обоснованы и достоверны.

5.4.3 Испытательная лаборатория (центр) при участии организации-разработчика должна провести экспертизу и испытания для подтверждения корректности доказательного материала, представленного в документе «Доказательство безопасности». Подтверждение обоснованности и корректности количественных показателей безопасности должно производиться с использованием расчетных методов.

5.4.4 Система ДЦ или ДК должна допускаться в эксплуатацию только при наличии положительного заключения от испытательной лаборатории (центра).

5.4.5 На этапе эксплуатации системы корректность выполнения требований безопасности к аппаратным и программным средствам должна оцениваться экспертными и расчетными методами по результатам мониторинга и статистических отчетов об отказах системы.

Сбор и обработка данных о безопасности и надежности эксплуатируемой системы ЖАТ осуществляются в соответствии с национальными стандартами и нормативными документами, действующими на территории государства, принявшего стандарт, по надежности в технике и сбору и обработке информации о надежности изделий в эксплуатации, с выделением при этом отказов (сбоев), вызванных отказами (сбоями) программного обеспечения.

Анализ последствий отказов (сбоев), вызванных отказами (сбоями) программного обеспечения, осуществляется в соответствии с национальными стандартами и нормативными документами, действующими на территории государства, принявшего стандарт[1)], по надежности в технике и методам оценки показателей надежности по экспериментальным данным.

[1)] В Российской Федерации действует РД 50-690—89 «Методические указания. Надежность в технике. Методы оценки показателей надежности по экспериментальным данным».

УДК 656.25:006.354 МКС 45.020

Ключевые слова: железнодорожная автоматика и телемеханика, диспетчерская централизация, диспетчерский контроль, безопасность движения железнодорожных поездов, критерии опасных отказов, требования безопасности, методы контроля

Редактор *Е.В. Яковлева*
Технические редакторы *В.Н. Прусакова, И.Е. Черепкова*
Корректор *Е.М. Поляченко*
Компьютерная верстка *Г.В. Струковой*

Сдано в набор 05.09.2019. Подписано в печать 24.09.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
gost.e-ecolog.ru gost.e-ecolog.ru

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru