научно-производственный центр
ПРОМЭЛЕКТРОНИКА

СОГЛАСОВАНО

Начальник Управления автоматики
и телемеханики ЦДИ –
филиала ОАО «РЖД»

_____ В.В. АНОШКИН
«___» _____ 2019 г.

УТВЕРЖДАЮ

Исполнительный директор
АО «НПЦ «Промэлектроника»

_____ А.В. НАГОВИЦЫН
«__05__» ____11____ 2019 г.

ВЫЧИСЛИТЕЛЬНЫЙ КОМПЛЕКС МИКРОПРОЦЕССОРНОЙ ЦЕНТРАЛИЗАЦИИ СТРЕЛОК И СИГНАЛОВ МПЦ-И

ЕРКФ.424359.002ТЗ

Дополнение №1 к Техническому заданию ТЗ 01502-0203-14

СОГЛАСОВАНО

Директор
ПКБ И ОАО «РЖД»
Согласовано письмом
№ИСХ-3992/ПКБЦ А.И. ЛИСИЦЫН
«_21_» ____10____ 2019 г.

Начальник опытно-
конструкторского отдела
АО «НПЦ «Промэлектроника»

_____ М.В. АБАКУМОВ
«_25_» ____10____ 2019 г.

СОГЛАСОВАНО

Первый заместитель
генерального директора
АО «НИИАС»
Согласовано письмом
№ 8573 Е.Н. РОЗЕНБЕРГ
«_28_» ____10____ 2019 г.

СОГЛАСОВАНО

Директор
ООО «Испытательный центр
«СЦБ-Эксперт»
_____ С.В. ПЛАСКОННЫЙ
«_20_» ____августа____ 2019 г.

научно-производственный центр
ПРОМЭЛЕКТРОНИКА

Утвержден
ЕРКФ.424359.002ТЗ-ЛУ

ВЫЧИСЛИТЕЛЬНЫЙ КОМПЛЕКС МИКРОПРОЦЕССОРНОЙ ЦЕНТРАЛИЗАЦИИ СТРЕЛОК И СИГНАЛОВ МПЦ-И

ЕРКФ.424359.002ТЗ

Дополнение №1 к Техническому заданию ТЗ 01502-0203-14

Разработал	Проверил	Нормоконтроль	Согласовано	Согласовано
Наринян	Абакумов	Частухина		
25.10.2019	25.10.19	25.10.19		

Версия	Листов
4А	44

ИСТОРИЯ ИЗМЕНЕНИЙ

Версия	Дата	Автор	Номера листов	Комментарий
1А	30.05.2019	Меледина А.М.	Все	Документ создан
2А	12.08.2019	Наринян С.В.	Все	Документ откорректирован по замечаниям главного конструктора Абакумова М.В.
3А	27.09 2019	Наринян С.В.	5,11,12,14,17,41	Документ откорректирован по замечаниям НИИАС письмо № 6937/исх-4285/НИИАС от 05.09.2019 и по замечаниям ПКБ И письмо № исх-3387/ПКБ И от 12.09.19
4А	17.10 2019	Наринян С.В.		Документ откорректирован по повторным замечаниям НИИАС письмо № 8189 от 15.10.2019
4А	05.11.2019			Документ утвержден

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ

В настоящем документе приняты следующие сокращения:

АРМ – автоматизированное рабочее место

ДСП – дежурный по станции

УБП – устройство бесперебойного питания

Мобильные технические средства – съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные носители), а также портативные вычислительные устройства и устройства связи с возможностью обработки информации

МПЦ-И – микропроцессорная централизация стрелок и сигналов МПЦ-И

ОКР – опытно-конструкторская работа

ПО – программное обеспечение

СОК – система объектных контроллеров

СПО – свободное программное обеспечение

СЦБ – сигнализация, централизация и блокировка

ТЗ – техническое задание

УБП – устройство бесперебойного электропитания

УКЦ – управляющий контроллер централизации

УСО – устройство сопряжения с объектами

ШН – электромеханик СЦБ

1 НАИМЕНОВАНИЕ, ШИФР ОКР, ОСНОВАНИЕ, СРОКИ ВЫПОЛНЕНИЯ ОКР

Наименование и обозначение: Вычислительный комплекс микропроцессорной централизации стрелок и сигналов МПЦ-И ЕРКФ.424359.002.

Шифр ОКР: МПЦ-И3+.

Плановые сроки выполнения ОКР: 2019 г.

Основание для разработки настоящего документа:

Настоящее Дополнение №1 к Техническому заданию ТЗ 01502-0203-14 «Вычислительный комплекс микропроцессорной централизации стрелок и сигналов МПЦ-И» (далее – Дополнение №1) разработано с целью:

- приведения требований к Микропроцессорной централизации стрелок и сигналов (МПЦ-И) (далее – системе, МПЦ-И) в соответствие с действующими нормативными документами;
- совершенствования системы согласно вновь предъявляемым требованиям к информационной и кибербезопасности;
- приведения требований к системе в соответствии с «Планом работ по импортозамещению и обеспечению кибербезопасности аппаратно-программных средств микропроцессорной централизации МПЦ-И Утвержденным заместителем генерального директора – главным инженером ОАО «РЖД» С.А. Кобзевым от 26.08.2019 г.
- упорядочения конструкторской и программной документации после изменения форм собственности и общероссийских идентификаторов предприятия-разработчика с заменой обозначения системы с ЭРИО.424359.001 на ЕРКФ.424359.002.

2 СОДЕРЖАНИЕ ИЗМЕНЕНИЙ

2.1 ЗАМЕНА НОРМАТИВНОЙ ДОКУМЕНТАЦИИ И ТРЕБОВАНИЙ К СИСТЕМЕ

Внести изменения в Техническое задание ТЗ 01502-0203-14 в соответствии с таблицей 1.

Таблица 1 - замена нормативной документации и требований к системе

Старая редакция	Новая редакция
1.1 НАИМЕНОВАНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ *1.1.2 Разработчик: Уральский государственный университет путей сообщения (УрГУПС), Научно-производственный центр "Промэлектроника"* *1.1.3 Заказчик: ГУП "Свердловская железная дорога"*	1.1 НАИМЕНОВАНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ *1.1.2 Разработчик: Научно-производственный центр "Промэлектроника"* *1.1.3 Разработка проводится АО «НПЦ «Промэлектроника» в инициативном порядке.*
1.1.5 *Порядок оформления и предъявления Заказчику результатов работ определяется в соответствии с ГОСТ 34.201-89 и настоящим техническим заданием.*	1.1.5 *Порядок оформления и предъявления Заказчику результатов работ определяется в соответствии с ГОСТ 33477 и СТО РЖД 08.021.*
1.3.4 Система МПЦ-И должна удовлетворять общим требованиям к электрической сигнализации, изложенным в следующих документах: • *"Правила технической эксплуатации железных дорог Российской Федерации" № ЦРБ-756 от 26.05.2000 г.* • *"Инструкция по сигнализации на железных дорогах Российской Федерации" № ЦРБ-757 от 26.05.2000 г.* • *"Инструкция по движению поездов и маневровой работе на железных дорогах Российской Федерации" № ЦД-790 от 16.10.2000 г.* • *"Нормы технологического проектирования устройств автоматики и телемеханики на федеральном железнодорожном транспорте" - НТП СЦБ/МПС-99 от 24.06.1999 г.*	1.3.4 Система МПЦ-И должна удовлетворять общим требованиям к электрической централизации, изложенным в следующих документах: • *ГОСТ 34012;* • ГОСТ 33894; • *Правила технической эксплуатации железных дорог Российской Федерации, утв. приказом Минтранса России от 21.12.2010 г. № 286;* • *Инструкция по сигнализации на железнодорожном транспорте Российской Федерации (Приложение №7 к ПТЭ), введена приказом Минтранса России от 04.06.2012 г. № 162;* • *Инструкция по движению поездов и маневровой работе на железнодорожном транспорте Российской Федерации (Приложение №8 к ПТЭ), введена приказом Минтранса России от 04.06.2012 г. № 162;* • *Свод правил СП 235.1326000.2015 "Железнодорожная автоматика и телемеханика. Правила проектирования", утв. приказом Минтранса России от 06.07.2015 г. № 205.*

Старая редакция	Новая редакция
2.1 ТРЕБОВАНИЯ К СИСТЕМЕ В ЦЕЛОМ *МПЦ-И должна удовлетворять общим требованиям к электрической централизации стрелок и сигналов, изложенным в Правилах технической эксплуатации железных дорог РФ.*	2.1 ТРЕБОВАНИЯ К СИСТЕМЕ В ЦЕЛОМ *МПЦ-И должна удовлетворять требованиям к системам железнодорожной автоматики и телемеханики на железнодорожных станциях, изложенным в ГОСТ 33894 и СТО РЖД 1.19.004.*
2.1.1.2.3 *Нижний уровень:* • вводно-коммуникационное оборудование для подключения аппаратуры к линиям связи и источникам питания; • аппаратно-программные устройства безопасного сопряжения (ввода/вывода) с управляемыми объектами (УСО); • пульт прямопроводного управления стрелками (стрелочные рукоятки, кнопки "ВК", контрольные индикаторы положения стрелок и состояния контролируемых участков и прочие органы контроля и резервного управления) для реализации режима "Резервное управление" при отказах АРМ ДСП или управляющего технологического контроллера централизации. Нижний уровень МПЦ-И должен обеспечивать взаимодействие со следующими подсистемами: • Контроля состояния объектов • Управления состоянием объектов	2.1.1.2.3 *Нижний уровень:* • вводно-коммуникационное оборудование для подключения аппаратуры к линиям связи и источникам питания; • аппаратно-программные устройства безопасного сопряжения (ввода/вывода) с управляемыми объектами (УСО) *при применении системы в варианте с релейным либо комбинированным интерфейсом*; • пульт прямопроводного управления стрелками (стрелочные рукоятки, кнопки "ВК", контрольные индикаторы положения стрелок и состояния контролируемых участков и прочие органы контроля и резервного управления) *при применении системы в варианте с релейным интерфейсом* для реализации режима "Резервное управление" при отказах АРМ ДСП или управляющего технологического контроллера централизации; • *система объектных контроллеров (СОК) для централизованного или распределенного управления объектами и контроля их состояния при применении системы в варианте с электронным либо комбинированным интерфейсом.* Нижний уровень МПЦ-И должен обеспечивать взаимодействие со следующими подсистемами: • Контроля состояния объектов • Управления состоянием объектов • *Диагностики аппаратуры МПЦ-И* • *Передачи и обработки информации*
2.1.1.3 Дополнительное оборудование, не входящее в состав МПЦ-И, но необходимое для ее функционирования: • постовые устройства питания: для защиты МПЦ-И от сбоев и потери информации при переключении фидеров питания, а также аварийном отключении электроснабжения должна применяться питающая установка с	2.1.1.3 Дополнительное оборудование, не входящее в состав МПЦ-И, но необходимое для ее функционирования: • постовые устройства электропитания: для защиты МПЦ-И от сбоев и потери информации при переключении фидеров питания, а также аварийном отключении электроснабжения должна применяться

Старая редакция	Новая редакция
контролем переключения фидеров и источника бесперебойного питания (ИБП); • *устройства контроля свободности участков пути, в качестве которых могут использоваться типовые рельсовые цепи либо аппаратура ЭССО ("Система контроля свободности участков пути методом счета осей" разработки НПЦ "Промэлектроника" УрГУПС, ТУ 01002-9911-1, сертификат РОСС RU.ЖА02.Н00011 № 0099129 от 20.08.2000 г.).* Увязка устройств контроля свободности с УКЦ должна производиться контактами путевых реле либо встроенными безопасными аппаратно-программными средствами сопряжения; • элементы управления напольными объектами - могут применяться типовые релейные блоки управления стрелками типа ПС или другие элементы с аналогичными характеристиками.	питающая установка с контролем переключения фидеров и устройством бесперебойного электропитания (УБП); • *устройства контроля свободности участков пути, в качестве которых могут использоваться типовые рельсовые цепи либо аппаратура систем счета осей.* Увязка устройств контроля свободности с УКЦ должна производиться контактами путевых реле, встроенными безопасными аппаратно-программными средствами сопряжения *либо средствами цифровых протоколов передачи ответственной информации*; • элементы управления напольными объектами - могут применяться интерфейсные реле свободного монтажа, типовые релейные блоки управления стрелками типа ПС, элементы с аналогичными *реле I-класса надежности характеристиками либо внешние безопасные устройства средствами цифровых протоколов передачи ответственной информации.*
2.1.1.6.5 Должна быть обеспечена возможность измерения параметров аналоговых сигналов с возможностью калибровки измерительных каналов. Точность измерений должна соответствовать требованиям, установленным в *п. 2.6 "Инструкции по обслуживанию устройств СЦБ" - № ЦШ 720.*	2.1.1.6.5 Должна быть обеспечена возможность измерения параметров аналоговых сигналов с возможностью калибровки измерительных каналов. Точность измерений должна соответствовать требованиям, установленным в *п. 2.7 Инструкции по техническому обслуживанию и ремонту устройств и систем сигнализации, централизации и блокировки, утв. распоряжением ОАО "РЖД" от 30.12.2015 № 3168р.*
	Дополнить раздел подпунктом: *2.1.1.6.8 Для обеспечения возможности применения системы в варианте с электронным интерфейсом вместо или в комбинации с УСО могут применяться системы объектных контроллеров, разработанные согласно дополнительных технических заданий с учетом всех требований к безопасности аппаратуры железнодорожной автоматики.*
2.1.1.7.7 Контрольная информация должна отображаться в виде условно-графических изображений на схематическом плане станции, согласно *ОСТ 32.111-98.*	2.1.1.7.7 Контрольная информация должна отображаться в виде условно-графических изображений на схематическом плане станции, в соответствии с требованиями

Старая редакция	Новая редакция
	СТО РЖД 1.19.005
2.1.2.7 *Сопряжение с напольными объектами* Управление напольными объектами должно производится через включенные последовательно одноименные выходы двух контроллеров УКЦ через безопасные УСО. Непосредственное управление стрелками и сигналами и контроль положения стрелки может осуществляться стандартными релейными схемами (сигнальными реле и блоками ПС-220 или аналогичные) либо другими элементами с аналогичными характеристиками, с возможностью передачи данной функции объектным контроллерам.	2.1.2.7 *Сопряжение с напольными объектами* Управление напольными объектами должно производится через одноименные выходы двух контроллеров УКЦ через безопасные УСО *либо средствами безопасных цифровых каналов передачи информации через СОК*. *При применении системы в варианте с релейным интерфейсом* непосредственное управление стрелками и сигналами и контроль положения стрелки должны осуществляться стандартными релейными схемами (сигнальными реле и блоками ПС-220 или аналогичными) либо другими элементами с аналогичными характеристиками. *При применении системы в варианте с электронным интерфейсом непосредственное управление стрелками и сигналами и контроль положения стрелки должен осуществляться объектными контроллерами СОК.*
2.1.5 Перспективы развития, модернизации МПЦ-И МПЦ-И должна иметь возможность развития и при необходимости обеспечивать расширение функционального набора и дополнение типов объектов контроля/управления. В дальнейшем при развитии МПЦ-И планируется мажоритарное (2 V 3) резервирование УКЦ.	2.1.5 Перспективы совершенствования, модернизации и модификации МПЦ-И МПЦ-И должна иметь возможность совершенствования и при необходимости обеспечивать расширение функционального набора и дополнение типов объектов контроля/управления. *Совершенствование функционала горячего резервирования системы должно выполняться в соответствии с частными техническими требованиями, установленными документом «Микропроцессорная централизация стрелок и сигналов МПЦ-И. Обеспечение горячего резервирования УКЦ. Технические требования. D.S424359-00205».*
2.3.1 Классификационные признаки по *ОСТ 32.146-2000* • *МПЦ-И должна являться изделием вида II (при применении по назначению может находиться в работоспособном, неработоспособном либо частично работоспособном состоянии, в которые может перейти в результате частичных отказов) непрерывного длительного применения (НПДП).*	2.3.1 Классификационные признаки по *ГОСТ 27.003:* • *по определенности назначения: объект конкретного назначения;* • *по режимам функционирования: изделие непрерывного длительного применения;* • *по возможным последствиям отказов: особо ответственное изделие, отказ которого может привести к последствиям катастрофического характера;*

Старая редакция	Новая редакция
• *МПЦ-И должна обеспечивать заданные уровни безопасности и надежности при применении по назначению во всех установленных условиях и режимах работы в соответствии со всеми принятыми моделями эксплуатации.* • *По характеру основных процессов, определяющих переход в предельное состояние, МПЦ-И должна относиться к физически стареющим изделиям.* • *Восстановление работоспособного состояния МПЦ-И после отказа в процессе эксплуатации должно производиться путем замены отказавших блоков на исправные из числа ЗИП.* • *По способу восстановления отказавшего блока МПЦ-И должна относиться к изделиям, ремонтируемым на предприятии-изготовителе или аттестованном Изготовителем сервисном центре после отказа в процессе эксплуатации.* • *По возможности и необходимости технического обслуживания МПЦ-И должна быть обслуживаемым изделием.* • *По возможности и необходимости контроля при применении по назначению МПЦ-И должна относиться к контролируемым изделиям с осуществлением контроля перед применением и непрерывно в процессе эксплуатации.* • *Аппаратно-программные средства МПЦ-И должны обеспечивать непрерывную круглосуточную работу с возможностью профилактического обслуживания без перерыва работы.* *МПЦ-И подлежит сертификации на соответствие требованиям надежности и безопасности в условиях воздействия механических нагрузок, климатических факторов и электромагнитных помех.*	• *по возможности восстановления работоспособного состояния после опасного отказа в процессе эксплуатации: восстанавливаемое изделие;* • *по характеру основных процессов, определяющих переход в опасное и предельное состояния: стареющее изделие;* • *по возможности и способу восстановления технического ресурса после отказа: изделие, ремонтируемое на предприятии-изготовителе или аттестованном Изготовителем сервисном центре после отказа в процессе эксплуатации;* • *по возможности технического обслуживания в процессе эксплуатации: изделие обслуживаемое;* • *по возможности (необходимости) проведения контроля: изделие, контролируемое перед применением и непрерывно контролируемое при применении;* • *по техническому исполнению: изделие с опасными отказами из-за возможных сбоев и отказов микроэлектронных элементов и средств вычислительной техники.* *МПЦ-И подлежит подтверждению соответствия требованиям технического регламента Таможенного союза ТР ТС 003/2011 «О безопасности инфраструктуры железнодорожного транспорта».*
2.3.6 МЕТОДЫ КОНТРОЛЯ *Методы определения и контроля показателей надежности должны устанавливаться в соответствии с конкретными условиями и требованиями ГОСТ 24.701-86, ГОСТ 27.301-83, ГОСТ 27.401-84, а также в соответствии с Программой обеспечения*	2.3.6 МЕТОДЫ КОНТРОЛЯ *Методы определения и контроля показателей надежности должны устанавливаться в соответствии с конкретными условиями и требованиями ГОСТ 24.701-86, ГОСТ 27.301-83, ГОСТ Р 27.403-2009, а также в соответствии с Программой обеспечения*

<table>
<tr><th>Старая редакция</th><th>Новая редакция</th></tr>
<tr><td>безопасности МПЦ-И. Уточнения либо изменения требований по надежности МПЦ-И на последующих стадиях разработки должны быть оформлены дополнением к настоящему техническому заданию (ТЗ) в соответствии с ГОСТ 24.201-85.</td><td>безопасности МПЦ-И. Уточнения либо изменения требований по надежности МПЦ-И на последующих стадиях жизненного цикла продукта должны быть оформлены дополнением к настоящему техническому заданию в соответствии с ГОСТ 34.602-89.</td></tr>
<tr><td>2.4.1 ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ
Безопасность программных и аппаратных средств должна отвечать требованиям ОСТ 32.17-92, ОСТ 32.19-92, ОСТ 3278-97, ОСТ 32.146-2000 и рекомендаций РТМ 32 ЦШ 1115842.01-94.
В соответствии с документом "Нормированные показатели безопасности электрической централизации на микропроцессорной основе", утвержденным в ЦШ МПС 05.01.1994 г. постовая аппаратура МПЦ-И должна удовлетворять следующим требованиям:
<table>
<tr><td>Измеритель</td><td>Интенсивность опасных отказов, λ, 1/ч</td></tr>
<tr><td>Станция</td><td>$1,8*10^{-7}$</td></tr>
<tr><td>Стрелка</td><td>$7,7*10^{-9}$</td></tr>
</table>
Для систем МПЦ, проектируемых на станциях с числом стрелок до N=22, в качестве условного измерителя для показателей безопасности выбирают станцию, для N>22 в качестве условного измерителя выбирают стрелку.</td><td>2.4.1 ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ
2.4.1.1 Безопасность функционирования МПЦ-И должна отвечать требованиям ГОСТ 33894 и СТО РЖД 1.19.004.
2.4.1.2 Безопасность аппаратных и программных средств МПЦ-И должна обеспечиваться применением при разработке методов и средств, выбор которых должен осуществляться в соответствии ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ IEC 61508-3, ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62279, СТО РЖД 08.021–2015, СТО РЖД 02.049–2014, СТО РЖД 02.051–2015.
2.4.1.3 Интенсивность опасных отказов системы не должна превышать:
• для станций до 22 стрелок $1 \cdot 10^{-7}$ 1/ч на станцию.
• для станций свыше 22 стрелок $1 \cdot 10^{-9}$ 1/ч на стрелку.</td></tr>
<tr><td>2.4.4 КРИТЕРИИ ОПАСНОГО ОТКАЗА
Признаки опасного состояния системы МПЦ-И:
• возникновение и накопление необнаруживаемых отказов хотя бы в одном из дублированных каналов;
• одновременный отказ обоих каналов обработки информации УКЦ вследствие идентичных одновременных сбоев или отказов технических средств;
• искажения в процессе обработки, приема или выдачи данных вследствие идентичных одновременных сбоев или отказов технических средств;
• искажения управляющих воздействий на объекты низовой и локальной автоматики, и выработка ложных контрольных и управляющих сигналов УКЦ вследствие идентичных одновременных сбоев или отказов технических средств, переводящих</td><td>2.4.4 КРИТЕРИИ ОПАСНОГО ОТКАЗА
Критериями опасных отказов МПЦ-И при реализации функций безопасности являются:
• невыполнение какого-либо условия безопасности при реализации МПЦ-И функций, указанных в п. 4.2 ГОСТ 33894;
• нарушение положений концепции безопасности, в соответствии с которой построены аппаратные и программные средства МПЦ-И;
• отклонение хотя бы одного показателя безопасности МПЦ-И за пределы установленных норм;
• выход показателей качества функционирования, влияющих на безопасность МПЦ-И, за пределы установленных норм в результате ее перехода в предельное состояние;
• выработка МПЦ-И ложных контрольных и управляющих сигналов, переводящих ее в</td></tr>
</table>

Старая редакция	Новая редакция
устройства ввода/вывода в опасное состояние.	*опасное состояние.*
2.4.6.1 ТРЕБОВАНИЯ ПО ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ *Аппаратура МПЦ-И должна соответствовать требованиям устойчивости к помехам в соответствии с ГОСТ Р 50656-2001, ОСТ 32.146-2000 и РД 32 ЦШ 1115842.05-95:* • *электромагнитная обстановка средней жесткости (аппаратура МПЦ-И расположена на посту централизации);* • *класс жесткости электромагнитной обстановки при эксплуатации МПЦ-И - II (непосредственно влияет на безопасность движения);* • *амплитуды испытательных воздействий - по ГОСТ Р 50656-2001;* • *критерий качества функционирования - С.*	2.4.6.1 ТРЕБОВАНИЯ ПО ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ *2.4.6.1.1 МПЦ-И должна устойчиво функционировать в условиях воздействия электромагнитных помех в соответствии с ГОСТ 33436.4-1.* *2.4.6.1.2 Критерий качества функционирования – А (для АРМ ШН допускается критерий качества функционирования – С)* *2.4.6.1.3 Уровень эмиссии индустриальных радиопомех, создаваемых системой, не должен превышать норм, установленных в ГОСТ 30804.6.4.*
2.4.6.2 ТРЕБОВАНИЯ ПО УСТОЙЧИВОСТИ И ПРОЧНОСТИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ МЕХАНИЧЕСКИХ НАГРУЗОК И КЛИМАТИЧЕСКИХ ФАКТОРОВ Оборудование МПЦ-И по устойчивости и прочности в условиях воздействия механических нагрузок и климатических факторов должно соответствовать требованиям *ОСТ 32.146-2000 (см. п. 2.7.1 настоящего ТЗ).*	2.4.6.2 ТРЕБОВАНИЯ ПО УСТОЙЧИВОСТИ И ПРОЧНОСТИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ МЕХАНИЧЕСКИХ НАГРУЗОК И КЛИМАТИЧЕСКИХ ФАКТОРОВ Оборудование МПЦ-И по устойчивости и прочности в условиях воздействия механических нагрузок и климатических факторов должно соответствовать требованиям *ГОСТ 34012-2016.*
2.4.7 ОБЩИЕ ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ 2.4.7.1 Показатели, обеспечивающие безопасность при монтаже, наладке, обслуживании и ремонте аппаратуры МПЦ-И по допустимым параметрам должны соответствовать требованиям *ГОСТ 24.104-85*, в частности: *2.4.7.1.1 Общие требования по электрической и механической безопасности - по Правилам эксплуатации электроустановок (ПУЭ), ГОСТ 12.2.007.0-85 и ГОСТ 25861-83, Правилам технической эксплуатации железных дорог РФ.* *2.4.7.1.2 Меры защиты от поражения электрическим током по ГОСТ 25881-83 и ГОСТ 12.1.019-79.* *2.4.7.1.3 Уровни шума и звуковой мощности в местах расположения персонала не должна превышать значений, установленных*	2.4.7 ОБЩИЕ ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ *2.4.7.1 Требования к безопасности при монтаже, наладке, обслуживании и ремонте аппаратуры МПЦ-И должны быть изложены в Руководстве по эксплуатации системы и соответствовать требованиям ГОСТ 33477 2015 и СТО РЖД 08.021-2015.* *2.4.7.2 Общие требования по электрической и механической безопасности - по ГОСТ 34012, Правилам эксплуатации электроустановок (ПУЭ), ГОСТ 12.2.007.0-85 и ГОСТ 25861-83, Правилам технической эксплуатации железных дорог РФ.* ***Пункты 2.4.7.1.2 - 2.4.7.1.4 исключить. Требования к уровням излучения, шума и вибрации изложить в п. 2.15 «Требования безопасности и охраны здоровья», раздел 2.3 настоящего документа.***

Старая редакция	Новая редакция
ГОСТ 12.1.003-83. *2.4.7.1.4 Общие требования к уровню вибрации по ГОСТ 12.1.012-78.*	
2.5.1 *Эргономические требования, регламентирующие организацию рабочего места, взаимное расположение средств отображения информации, органов управления и средств связи в пределах рабочего места должны соответствовать ГОСТ 21889-76, ГОСТ 21.958-76, ГОСТ 22269-76, ГОСТ 23000-76, ГОСТ Р 50923-96, ГОСТ Р 50933-96, ГОСТ Р 50948-96 и ГОСТ Р 51341-99, СанПиН 2.2.2.542-96, а также ведомственным нормативным документам.* 2.5.2 *Требования технической эстетики к устройствам МПЦ-И должны соответствовать ГОСТ 24.750-80.* 2.5.3 Надписи на экранах мониторов и на блоках и модулях должны выполняться печатными буквами на русском языке. Все блоки и модули должны иметь таблички с указанием их типа. 2.5.4 *Условные графические изображения и индикация должны соответствовать требованиям ОСТ 32.111-98.*	2.5.1 *Эргономические требования, регламентирующие организацию рабочего места, взаимное расположение средств отображения информации, органов управления и средств связи в пределах рабочего места должны соответствовать ГОСТ 21889-76, ГОСТ 21.958-76, ГОСТ 22269-76, ГОСТ 23000-76, ГОСТ Р 50923-96, ГОСТ Р 50933-96, ГОСТ Р 50948-2001 и ГОСТ Р 51341-99, СанПиН 2.2.2/2.4.1340-03, а также ведомственным нормативным документам.* 2.5.2 *Требования технической эстетики к устройствам МПЦ-И должны соответствовать ГОСТ 24750-81.* 2.5.3 Надписи на экранах мониторов и на блоках и модулях должны выполняться печатными буквами на *официальном государственном* языке. Все блоки и модули должны иметь таблички с указанием их типа. 2.5.4 *Условные графические изображения и индикация должны соответствовать требованиям СТО РЖД 1.19.005.*
2.6.1 УСЛОВИЯ ЭКСПЛУАТАЦИИ Технические средства системы МПЦ-И с обеспечением заданных технических показателей должны эксплуатироваться в отапливаемых помещениях (постовое оборудование). 2.6.1.1 Классификация узлов МПЦ-И по воздействию климатических факторов согласно *ОСТ 32.146-2000*:* 2.6.1.2 Классификация узлов МПЦ-И по воздействию механических факторов при применении по назначению согласно *ОСТ 32.146-2000*:* *содержимое таблиц п.2.6.1.1 и п.2.6.1.2 без изменений	2.6.1 УСЛОВИЯ ЭКСПЛУАТАЦИИ Технические средства системы МПЦ-И с обеспечением заданных технических показателей должны эксплуатироваться в отапливаемых помещениях (постовое оборудование). 2.6.1.1 Классификация узлов МПЦ-И по воздействию климатических факторов согласно *ГОСТ 34012-2016*:* 2.6.1.2 Классификация узлов МПЦ-И по воздействию механических факторов при применении по назначению согласно *ГОСТ 34012-2016:** *содержимое таблиц п. 2.6.1.1 и п. 2.6.1.2 без изменений
2.6.2.5 В процессе обслуживания и ремонта узлов МПЦ-И может допускаться их отключение с обеспечением: • условий безопасности движения поездов; • *Инструкции по техническому обслуживанию устройств сигнализации, централизации и блокировки.*	2.6.2.5 В процессе обслуживания и ремонта узлов МПЦ-И может допускаться их отключение с обеспечением: • условий безопасности движения поездов; • *Инструкции по техническому обслуживанию и ремонту устройств и систем сигнализации, централизации и*

Старая редакция	Новая редакция
	блокировки, утв. распоряжением ОАО "РЖД" от 30.12.2015 № 3168р.
2.6.2.7.1 Оборудование МПЦ-И размещается в зданиях с соблюдением требований, содержащихся в технической и эксплуатационной документации, а также в соответствии с санитарно-гигиеническими нормами *СанПиН 2.2.2.542-96.*	2.6.2.7.1 Оборудование МПЦ-И размещается в зданиях с соблюдением требований, содержащихся в технической и эксплуатационной документации, а также в соответствии с санитарно-гигиеническими нормами *СанПиН 2.2.2/2.4.1340-03.*
2.7 *ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА* *2.7.1 Несанкционированный доступ к информации должен исключаться особенностями построения ПО, применением специальных информационных шлюзов и фильтров, а также организационными мерами.* *2.7.2 Доступ к информации и управлению должен быть разрешен только лицам, занимающимся эксплуатацией и обслуживанием. Должна быть предусмотрена система идентификации персонала.* *2.7.3 По желанию Заказчика несанкционированный доступ к системе может исключаться вводом паролей и/или дополнительных индивидуальных аппаратных средств (ключей), блокирующих работу АРМ.* *2.7.4 Количественные показатели степени защиты от несанкционированного доступа и воздействий из локальной сети предприятия должны быть определены на этапе сертификации системы.* *2.7.5 Аппаратура МПЦ-И должна размещаться в запираемых помещениях.* *2.7.6 Должны быть защищены от несанкционированного доступа и изменения следующие виды информации системы:* • *исполнительные программные модули системы в УКЦ - встроенными средствами паролевой защиты УКЦ;* • *архивные файлы - встроенными средствами операционной системы на базе Windows NT, Системы Управления Базами Данных и встроенной системой безопасности сервера баз данных;* • *информационные шлюзы в локальной сети предприятия - встроенными средствами операционной системы на базе Windows NT и встроенной системой безопасности АРМов и*	2.7 *ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРБЕЗОПАСНОСТИ* ***Данный раздел переработан в соответствии с требованиями СТО РЖД 02.049.*** ***Заголовок 2.7 переименовать.*** ***Подпункты 2.7.1 - 2.7.6 исключить*** ***Взамен включить требования, указанные в разделе 2.2 настоящего документа.***

Старая редакция	Новая редакция
сервера приложений.	
2.10.7 В компьютерных элементах МПЦ-И должны применяться современные операционные системы и структурное построение ПО, позволяющее при необходимости заменять отдельные его части.	2.10.7 В компьютерных элементах МПЦ-И должны применяться *российские операционные системы и свободное программное обеспечение (СПО), позволяющее при необходимости верифицировать, модифицировать или* заменять отдельные его части. *Операционные системы, применяемые в аппаратуре МПЦ-И, непосредственно влияющие на безопасность системы, должны быть сертифицированы уполномоченным органом на функциональную и информационную безопасность.*
2.12.4 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ	2.12.4 ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ ***Дополнить раздел подпунктом:*** *2.13.4.9 Качество ПО МПЦ-И должно соответствовать требованиям, ГОСТ Р 52980-2008, СТО РЖД 02.051.* *Оценка качества ПО МПЦ-И должна производиться в соответствии с ГОСТ Р ИСО/МЭК 9126.*
2.12.5.1 Надежность, технические, эксплуатационные и функциональные характеристики средств МПЦ-И должны удовлетворять соответствующим пунктам *ОСТ 32.146-2000.*	2.12.5.1 Надежность, технические, эксплуатационные и функциональные характеристики средств МПЦ-И должны удовлетворять соответствующим пунктам *ГОСТ 34012.*
2.12.8.1 Функционирование МПЦ-И должно учитывать действующие *Правила технической эксплуатации железных дорог РФ и Инструкцию по движению поездов и маневровой работе на железных дорогах.*	2.12.8.1 Функционирование МПЦ-И должно учитывать действующие *Правила технической эксплуатации железных дорог РФ.*
3 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО СОЗДАНИЮ (РАЗВИТИЮ) СИСТЕМЫ	***Этапы выполнения ОКР представлены в разделе 3 настоящего документа.***
4 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ	***Порядок выполнения и приемки этапов ОКР представлен в разделе 4 настоящего документа.***
5 ПОДГОТОВКА СТАНЦИИ ВНЕДРЕНИЯ К ВВОДУ ОПЫТНОГО ОБРАЗЦА СИСТЕМЫ В ДЕЙСТВИЕ 5.1 Для подготовки станции внедрения к вводу опытного образца в действие, согласно *"Инструкции о порядке проведения эксплуатационных и приемочных испытаний опытных образцов аппаратуры железнодорожной автоматики и телемеханики (устройств СЦБ)" № ЦШ/604* необходимо:	5 ПОДГОТОВКА СТАНЦИИ ВНЕДРЕНИЯ К ВВОДУ ОПЫТНОГО ОБРАЗЦА СИСТЕМЫ В ДЕЙСТВИЕ 5.1 Для подготовки станции внедрения к вводу опытного образца в действие, согласно *СТО РЖД 08.021* необходимо: • Разработать и утвердить Инструкцию о порядке пользования устройствами СЦБ на станции внедрения. • Разработать и утвердить инструкцию о технической эксплуатации системы МПЦ-И на

Старая редакция	Новая редакция
• Разработать и утвердить Инструкцию о порядке пользования устройствами СЦБ на станции внедрения. • Разработать и утвердить инструкцию о технической эксплуатации системы МПЦ-И на станции внедрения. Примечание: данные инструкции должны разрабатываться предприятием станции внедрения совместно с разработчиком. • Организовать обучение оперативного и оперативно-технического персонала станции внедрения. Примечание: обучение для ДСП по курсу "Пользование системой МПЦ-И", для электромехаников СЦБ по курсу "Эксплуатация системы МПЦ-И". 5.2 До ввода системы в опытную эксплуатацию на станции внедрения должна быть следующая документация (с учетом требований *ОСТ 32.91-97* в части обеспечения условий безопасности движения ЖТ)	станции внедрения. Примечание: данные инструкции должны разрабатываться предприятием станции внедрения совместно с разработчиком. • Организовать обучение оперативного и оперативно-технического персонала станции внедрения. Примечание: обучение для ДСП по курсу "Пользование системой МПЦ-И", для электромехаников СЦБ по курсу "Эксплуатация системы МПЦ-И". 5.2 До ввода системы в опытную эксплуатацию на станции внедрения должна быть документация в соответствии с *СТО РЖД 08.021*
7 НОРМАТИВНЫЕ ССЫЛКИ	***Нормативные ссылки представлены в Приложении А к настоящему документу.***

2.2 ВНОВЬ ВВОДИМЫЕ ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРБЕЗОПАСНОСТИ

Изложить п. 2.7 Технического задания ТЗ 01502-0203-14 в соответствии с таблицей 2.

Таблица 2 - требования информационной безопасности и кибербезопасности

Новый пункт	Новая редакция
2.7	ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРБЕЗОПАСНОСТИ МПЦ-И должна отвечать требованиям информационной и кибербезопасности в соответствии с требованиями СТО РЖД 08.021-2015, . СТО РЖД 02.051-2015 и «Положением о порядке проведения работ по обеспечению кибербезопасности микропроцессорных систем управления ОАО «РЖД», утвержденным Старшим вице-президентом ОАО «РЖД» В.А. Гапановичем 19.09.2014 и «Плана работ по импортозамещению и обеспечению кибербезопасности аппаратно-программных средств МПЦ-И» Утверждённом заместителем генерального директора - главным инженером ОАО «РЖ Д » С.А. Кобзевым от 26.08.2019 г.
2.7.1	**Требования по отсутствию в программном обеспечении МПЦ-И недекларированных возможностей**

Новый пункт	Новая редакция
2.7.1.1	ПО МПЦ-И не должно иметь свойств и характеристик, не описанных в технической документации на программные средства (недекларированных возможностей).
2.7.1.2	В части контроля отсутствия недекларированных возможностей МПЦ-И должна относиться к четвёртому уровню контроля, который является достаточным для ПО, используемого при защите конфиденциальной информации, в соответствии с документом ФСТЭК России «Требования к уровню доверия» от 01.06.2019 г.
2.7.2	**Требования к классам защищенности в отношении информационной безопасности и кибербезопасности**
2.7.2.1	Программные средства МПЦ-И должны обеспечивать защищенность информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации. МПЦ-И не предназначена для использования в открытых сетях общего пользования без использования дополнительных средств защиты информации.
2.7.2.2	В части обеспечения защиты информации МПЦ-И должна относиться ко второму классу защищённости (К2) в соответствии с Приказом ФСТЭК России от 14 марта 2014 г. №31 «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
2.7.2.3	В части защищённости средств вычислительной техники МПЦ-И от несанкционированного доступа система должна относиться к пятому классу защищённости, в соответствии с СТО РЖД 1.19.004 и Руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» от 30 марта 1992 г.
2.7.2.4	В части защищённости ПО МПЦ-И при межсетевом взаимодействии со смежными системами ЖАТ и при предоставлении временного удалённого доступа к системе, в том числе, с использованием мобильных устройств, при проведении пуско-наладочных работ и испытаний МПЦ-И, система должна относиться к пятому классу защищённости, в соответствии с Руководящим документом «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» от 25 июля 1997 г.
2.7.3	**Меры защиты информации и обеспечения кибербезопасности** Организационные и технические меры защиты информации и обеспечения кибербезопасности, реализуемые в МПЦ-И, должны соответствовать требованиям Приказа №31 ФСТЭК России от 14 марта 2014 г.
2.7.3.1	***Требования к идентификации и аутентификации (ИАФ)***

Новый пункт	Новая редакция
2.7.3.1.1	*Разработка политики идентификации и аутентификации* В системе должны быть обеспечены идентификация и аутентификация пользователей системы, и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. Аутентификация пользователей должна осуществляться с использованием паролей. Требования к характеристикам пароля должны быть установлены в организационно-распорядительной документации.
2.7.3.1.2	*Идентификация и аутентификация пользователей и инициируемых ими процессов* В системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация устройств (технических средств). Должен быть определен перечень типов устройств, используемых в системе и подлежащих идентификации и аутентификации до начала информационного взаимодействия.
2.7.3.1.3	*Управление идентификаторами* Система должна обеспечивать возможность управления идентификаторами, в том числе: – формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство; – присвоение идентификатора пользователю и (или) устройству; – предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного периода времени; – блокирование идентификатора пользователя после установленного оператором времени неиспользования.
2.7.3.1.4	*Управление средствами аутентификации* В системе должны быть реализованы функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в системе, обеспечивающие: – изменение аутентификационной информации (средств аутентификации), заданных их производителями; – установление характеристик пароля (при использовании в системе механизмов аутентификации на основе пароля): – блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации; – обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной оператором. В системе должны быть установлены следующие характеристики средств аутентификации (механизм пароля): а) задание минимальной сложности пароля с требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов; в) задание максимального времени действия пароля; д) запрет на использование пользователями заданного числа последних использованных паролей при создании новых паролей.

Новый пункт	Новая редакция
2.7.3.1.5	*Идентификация и аутентификация внешних пользователей* В системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками.
2.7.3.1.6	*Защита аутентификационной информации при передаче* Для передачи аутентификационной информации должны использоваться защищенные протоколы.
2.7.3.2	***Требования к управлению доступом (УПД)***
2.7.3.2.1	*Управление учетными записями пользователей* В системе должны быть реализованы следующие функции управления учетными записями пользователей: – заведение, модификация, активация, блокирование и уничтожение учетных записей пользователей; – определение типа учетной записи; – объединение учетных записей в группы; – пересмотр и, при необходимости, корректировка учетных записей пользователей – предоставление пользователям прав доступа к объектам доступа системы, основываясь на задачах, решаемых пользователями в системе и взаимодействующими с ней информационными системами.
2.7.3.2.2	*Реализация политик управления доступа* Для управления доступом субъектов доступа к объектам доступа в системе должны быть назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа. Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа. Правила разграничения доступа должны: – обеспечивать управление доступом субъектов при входе в систему; – обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам; – управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением.

Новый пункт	Новая редакция
2.7.3.2.3	*Доверенная загрузка* В системе должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники системы на этапе его загрузки. Доверенная загрузка должна обеспечивать: – блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы; – контроль доступа пользователей к процессу загрузки операционной системы; – контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.
2.7.3.2.4	*Разделение полномочий (ролей) пользователей* Система должна обеспечивать возможность разделения полномочий (ролей) пользователей в соответствии с их должностными обязанностями (функциями), и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).
2.7.3.2.5	*Назначение минимально необходимых прав и привилегий* В системе должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями. Должны быть однозначно определены должностные обязанности (функции) и объекты доступа, в отношении которых установлен наименьший уровень привилегий.
2.7.3.2.6	*Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему* В системе должно предусматриваться ограничение количества неуспешных попыток входа в систему с увеличенным таймаутом до следующей попытки, кроме доступа в систему оперативного и эксплуатационного персонала с АРМ ДСП и АРМ ШН.
2.7.3.2.7	*Блокирование сеанса доступа пользователя при неактивности* В системе должно предусматриваться блокирование сеанса доступа пользователя после установленного периода времени его бездействия (неактивности) в системе, кроме сеансов оперативного и эксплуатационного персонала с АРМ ДСП и АРМ ШН.
2.7.3.2.8	*Управление действиями пользователей до идентификации и аутентификации* В системе должен быть предусмотрен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.

Новый пункт	Новая редакция
2.7.3.2.9	*Реализация защищенного удаленного доступа* Должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) к объектам доступа системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа). Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает: – установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы; – ограничение на использование удаленного доступа в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с п. 2.7.3.2.2; – предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций); – мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы; – контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа системы до начала информационного взаимодействия с системой.
2.7.3.2.10	*Контроль доступа из внешних информационных (автоматизированных) систем* В системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках системы, включающее: – фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными Заказчиком; – разрешение передачи информации в системе только по маршруту, установленному Заказчиком; – изменение (перенаправление) передачи информации в случаях, установленных Заказчиком; – запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных Заказчиком; – однонаправленную передачу информации между сегментами внутри системы и (или) систем разных классов защищенности с использованием аппаратных средств в случаях, установленных Заказчиком. В МПЦ-И передача данных в соседнюю информационную систему должна идти по строго ограниченному каналу. Передача информации через сеть Интернет не предусматривается.
2.7.3.3	***Требования к ограничению программной среды (ОПС)***

Новый пункт	Новая редакция
2.7.3.3.1	*Управление установкой (инсталляцией) компонентов программного обеспечения* В системе должны быть предусмотрены механизмы управления установкой (инсталляцией) компонентов программного обеспечения: – определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке после загрузки операционной системы; – выбор конфигурации устанавливаемых компонентов программного обеспечения; – контроль над установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов); – определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации.
2.7.3.4	***Требования к защите машинных носителей информации (ЗНИ)***
2.7.3.4.1	*Учет машинных носителей информации* В системе должны быть предусмотрены механизмы, позволяющие осуществлять контроль подключения и ввода (вывода) информации на машинные носители информации.
2.7.3.4.2	*Управление физическим доступом к машинным носителям информации* Порядок и правила доступа к машинным носителям информации должны регламентироваться в организационно-распорядительных документах по защите информации.
2.7.3.4.3	*Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации* Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать: – определение интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в системе; – определение категорий пользователей, которым предоставлен доступ к разрешенным к использованию интерфейсов ввода (вывода); – принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода); – контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода).

Новый пункт	Новая редакция
2.7.3.4.4	*Контроль подключения машинных носителей информации* Контроль подключения и ввода (вывода) информации на машинные носители информации должен предусматривать: – определение типов носителей информации, подключение которых разрешено; – определение категорий пользователей, которым предоставлены полномочия по подключению и вводу (выводу) информации на машинные носители; – запрет действий по подключению и вводу (выводу) информации для пользователей, не имеющих полномочий на ввод (вывод) информации на машинные носители информации, и на носители информации, на которые запрещен ввод (вывод) информации; – регистрацию действий пользователей и событий по подключению и вводу (выводу) информации на машинные носители информации.
2.7.3.4.5	*Уничтожение (стирание) информации на машинных носителях информации* Процедура уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации должны регламентироваться в организационно-распорядительных документах по защите информации.
2.7.3.5	***Требования к аудиту безопасности (АУД)***
2.7.3.5.1	*Инвентаризация информационных ресурсов* Требования и процедуры инвентаризации информационных ресурсов должны регламентироваться в организационно-распорядительных документах по защите информации.
2.7.3.5.2	*Генерирование временных меток и (или) синхронизация системного времени* В системе должна осуществляться синхронизация системного времени. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в системе достигается посредствам применения внутренних системных часов информационной системы.

Новый пункт	Новая редакция
2.7.3.5.3	*Регистрация событий безопасности* В системе должны быть определены события безопасности, подлежащие регистрации, сроки их хранения, а также механизмы, позволяющие регистрировать события безопасности. Регистрации подлежат как минимум следующие события: – вход (выход), а также попытки входа субъектов доступа в систему и загрузки (останова) операционной системы; – подключение машинных носителей информации и вывод информации на носители информации; – запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации; – попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа; – попытки удаленного доступа к системе. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности. При регистрации входа (выхода) субъектов доступа в систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум включать дату и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа. В системе должны осуществляться централизованные сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения информации о событиях безопасности.
2.7.3.5.4	*Защита информации о событиях безопасности* В системе должна обеспечиваться защита информации о событиях безопасности. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.
2.7.3.5.5	*Мониторинг безопасности* В системе должны быть предусмотрены механизмы, позволяющие осуществлять мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

Новый пункт	Новая редакция
2.7.3.5.6	*Реагирование на сбои при регистрации событий безопасности* В системе должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти. Реагирование на сбои при регистрации событий безопасности должно предусматривать: – предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации и достижении предела или переполнения объема (емкости) памяти) при регистрации событий безопасности; – реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части элементов системы, запись поверх устаревших хранимых записей событий безопасности.
2.7.3.5.7	*Проведение внутренних аудитов* В системе должны быть предусмотрены механизмы регистрации событий, относящихся к возможным нарушениям безопасности. Механизмы регистрации должны предоставлять уполномоченным лицам с учетом их ролей возможность полного или выборочного ознакомления с информацией о произошедших событиях.
2.7.3.6	***Требования к антивирусной защите (АВЗ)*** Система должна надежно функционировать без использования внешних средств антивирусной защиты. Защита от вирусов должна обеспечиваться защищенными каналами передачи данных, ограничением использования съемных носителей, использованием ОС, для которых антивирусная защита не требуется.
2.7.3.7	***Требования к предотвращению вторжений (компьютерных атак) (СОВ)***
2.7.3.7.1	*Обнаружение и предотвращение компьютерных атак* В системе должны быть предусмотрены механизмы обнаружения (предотвращения) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений. Системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак. Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе системы (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах), определяемых оператором. Права по управлению (администрированию) системами обнаружения вторжений должны предоставляться только уполномоченным должностным лицам.

Новый пункт	Новая редакция
2.7.3.7.2	*Обновление базы решающих правил* Механизмы обнаружения вторжений должны иметь возможность обновления правил выявления, нормализации и корреляции событий информационной безопасности, и атак.
2.7.3.8	***Требования к обеспечению целостности (ОЦЛ)***
2.7.3.8.1	*Контроль целостности программного обеспечения* Все устройства, содержащие программное обеспечение, должны периодически программно проверять его целостность. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать: – контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы; – контроль целостности компонентов программного обеспечения (за исключением средств защиты информации) по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы системы; – обеспечение физической защиты технических средств системы.
2.7.3.8.2	*Контроль данных, вводимых в систему* Задание команд пользователем должно осуществляться путем выбора из предложенных вариантов команд в графическом пользовательском интерфейсе. Вводимые пользователем данные не должны интерпретироваться как команды.
2.7.3.8.3	*Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях* В системе должен осуществляться контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях. Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях должен предусматривать: – определение типов ошибочных действий пользователей, которые потенциально могут привести к нарушению безопасности информации в системе; – генерирование сообщений для пользователей об их ошибочных действиях и о возможности нарушения безопасности информации в системе для корректировки действий пользователей; – регистрация информации об ошибочных действиях пользователей, которые могут привести к нарушению безопасности информации в системе, в журналах регистрации событий безопасности; – предоставление доступа к сообщениям об ошибочных действиях пользователей только администраторам.

Новый пункт	Новая редакция
2.7.3.9	***Требования к обеспечению доступности (ОДТ)***
2.7.3.9.1	*Использование отказоустойчивых технических средств* Система должна быть построена с использованием отказоустойчивых технических средств.
2.7.3.9.2	*Резервирование средств и систем* Система должна быть построена с соблюдением принципов резервирования технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы.
2.7.3.9.3	*Контроль безотказного функционирования средств и систем* В системе должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.
2.7.3.9.4	*Резервное копирование информации* В системе должны быть предусмотрены механизмы, позволяющие осуществлять с установленной периодичностью резервное копирование информации на резервные машинные носители информации.
2.7.3.9.5	*Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях* Программное обеспечение системы должно быть записано на постоянных запоминающих устройствах (жёстких магнитных, твердотельных, СЭ/ЭУЭ дисках и т.д.) и сохраняться при выключении питания. В комплект поставки системы должны входить резервные копии программного обеспечения, обеспечивающие возможность оперативного восстановления эксплуатационным штатом функционирования системы при повреждении загруженного в систему программного обеспечения.
2.7.3.9.6	*Мониторинг состояния и качества вычислительных ресурсов (мощностей)* Система должна осуществлять мониторинг состояния и качества вычислительных ресурсов в рамках функционирования подсистемы диагностики.
2.7.3.10	***Требования к защите технических средств и систем (ЗТС)***
2.7.3.10.1	*Организация контролируемой зоны* Технические средства системы должны обеспечивать требуемый уровень защиты от несанкционированного доступа и внешних воздействий. Размещение технических средств системы должно исключать доступ к ним лиц, не имеющих на это полномочий.

Новый пункт	Новая редакция
2.7.3.10.2	*Управление физическим доступом* Технические средства системы должны оснащаться аппаратными средствами контроля физического доступа к ним. Контроль и управление физическим доступом должны предусматривать: – определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены; – санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены; – учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.
2.7.3.10.3	*Защита от внешних воздействий* Защита программного обеспечения от внешних влияний должна обеспечиваться аппаратными и программными средствами, такими как защита корпусов и каналов передачи данных от электростатических и механических воздействий, резервные копии, проверка контрольных сумм с возможностью перехода на резервный комплект оборудования. Защита системы от внешних воздействий должна предусматривать: – выполнение норм и правил пожарной безопасности; – выполнение норм и правил устройства и технической эксплуатации электроустановок, а также соблюдение параметров электропитания и заземления технических средств; – обеспечение необходимых для эксплуатации технических средств температурно-влажностного режима и условий по степени запыленности воздуха.
2.7.3.11	***Требования к защите системы и ее компонентов (ЗИС)***
2.7.3.11.1	*Разделение функций по управлению (администрированию) системой с иными функциями* В системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации. Разделение функциональных возможностей должно обеспечиваться на физическом и логическом уровне путем выделения части программнотехнических средств системы, реализующих функциональные возможности по управлению (администрированию) системой и управлению (администрированию) системой защиты информации.

Новый пункт	Новая редакция
2.7.3.11.2	*Защита периметра системы* В системе должна осуществляться защита периметра (физических и (или) логических границ) при ее взаимодействии со смежными системами или другими информационными системами, предусматривающая: – управление (контроль) входящими в систему и исходящими из нее информационными потоками на физической и (или) логической границе системы (сегментах информационных систем); – обеспечение взаимодействия системы и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).
2.7.3.11.3	*Эшелонированная защита системы* Защита системы не должна быть сосредоточена на одном уровне или устройстве. Должно быть выполнено распределение средств защиты на разных уровнях системы и разных устройствах для обеспечения более высокого качества защищенности системы.
2.7.3.11.4	*Сегментирование системы* Принципы сегментирования системы должны определяться с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации и должны заключаться в снижении вероятности реализации угроз и (или) их локализации в рамках одного сегмента.
2.7.3.11.5	*Сокрытие архитектуры и конфигурации системы* В случае возникновения отказов (сбоев) в системе защиты информации, должен осуществляться перевод системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации. Перевод системы или ее устройств (компонентов) в заранее определенную конфигурацию должен обеспечивать защиту информации при наступлении (возникновении) отказов (сбоев) в функционировании системы или ее сегментов, которые могут привести к нарушению конфиденциальности, целостности и (или) доступности этой информации.
2.7.3.11.6	*Защита неизменяемых данных* В системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации. Защита должна обеспечиваться за счет ограничения доступа пользователей к частям диска, на которых размещены эти данные.
2.7.3.11.7	*Защита информации при ее передаче по каналам связи* В системе должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

Новый пункт	Новая редакция
2.7.3.11.8	*Обеспечение доверенных каналов, маршрутов* В системе должны обеспечиваться доверенные маршруты передачи данных между администратором (пользователем) и средствами защиты информации (функциями безопасности средств защиты информации).
2.7.3.11.9	*Обеспечение подлинности сетевых соединений* В системе должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»). В системе должна осуществляться передача, сопоставление (сравнение) атрибутов безопасности (меток безопасности) с информацией, которой она обменивается с иными (внешними) информационными системами.
2.7.3.11.10	*Защита от угроз отказа в обслуживании (DOS, DDOS-атак)* В системе должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании этой системы.
2.7.3.11.11	*Управление сетевыми соединениями* Защита информации должна обеспечиваться путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.
2.7.3.11.12	*Защита информации при использовании мобильных устройств* Должна быть осуществлена защита применяемых в системе мобильных технических средств.
2.7.3.12	***Требования к реагированию на компьютерные инциденты (ИНЦ)***
2.7.3.12.1	*Выявление компьютерных инцидентов* В системе должны быть настроены политики аудита с целью регистрации этих событий в системных журналах ОС. В системе должен быть предусмотрен сбор и первичная обработка информации, поступающей от источников событий информационной безопасности.
2.7.3.13	***Требования к управлению конфигурацией (УКФ)***
2.7.3.13.1	*Управление изменениями* В МПЦ-И должно быть установлено только программное обеспечение, входящее в состав ПО комплекса. Установка дополнительного ПО недопустима.
2.7.3.13.2	*Установка (инсталляция) только разрешенного к использованию программного обеспечения* В системе должна быть обеспечена установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов. Установка (инсталляция) в системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора.
2.7.3.14	***Требования к управлению обновлениями программного обеспечения (ОПО)***
2.7.3.14.1	*Поиск, получение обновлений программного обеспечения от доверенного источника* Правила и процедуры контроля установки обновлений программного обеспечения должны регламентироваться в организационно-распорядительных документах.

Новый пункт	Новая редакция
2.7.3.14.2	*Контроль целостности обновлений программного обеспечения* На уровне системного ПО в МПЦ-И должен использоваться механизм защиты от непреднамеренных искажений при хранении или считывании данных (контроль исправности носителя и аппаратно-программных средств). Загрузка ПО с неправильной фиксированной контрольной суммой должна блокироваться системой.
2.7.3.14.3	*Тестирование обновлений программного обеспечения* Проверка обновления ОС на предмет их совместной работы с ПО МПЦ-И осуществляется разработчиком ПО МПЦ-И. После этой проверки обновление может быть установлено на компьютерах системы МПЦ-И.
2.7.3.14.4	*Установка обновлений программного обеспечения* Установка обновлений программного обеспечения должна производиться из официальных источников производителя ОС при изготовлении системы, а также при проведении сервисного обслуживания.
2.7.3.15	***Требования к обеспечению действий в нештатных ситуациях (ДНС)***
2.7.3.15.1	*Разработка плана действий в нештатных ситуациях* Для обеспечения возможности восстановления программного обеспечения в системе должны быть разработаны соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций.
2.7.3.15.2	*Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций* Система должна быть построена с соблюдением принципов резервирования технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы.
2.7.3.15.3	*Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций* В комплект поставки системы должны входить резервные копии ПО, обеспечивающие возможность оперативного восстановления эксплуатационным штатом функционирования системы при повреждении загруженного в систему ПО.

Новый пункт	Новая редакция
2.7.3.15.4	*Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций* Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать: – восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения; – восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации; – возврат системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей системы, определенных разработчиком системы, позволяющих решать задачи по обработке информации. Должны применяться компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно. Правила и процедуры восстановления (в том числе планы по действиям персонала, порядок применения компенсирующих мер) должны отражаться в организационно-распорядительных документах по защите информации. Должно обеспечиваться восстановление отдельных функциональных возможностей системы с применением резервированного программного обеспечения зеркальной системы (сегмента системы, технического средства, устройства).
2.7.3.16	***Требования к информированию и обучению персонала (ИПО)*** Порядок информирования, обучения и контроля осведомленности пользователей системы и обслуживающего персонала об угрозах безопасности информации и о правилах безопасной работы должны регламентироваться в организационно-распорядительных документах на систему.

2.3 ВНОВЬ ВВОДИМЫЕ ТРЕБОВАНИЯ К СТРУКТУРЕ ТЗ

Внести новые разделы в Техническое задание ТЗ 01502-0203-14 в соответствии с таблицей 3.

Таблица 3 – требования к структуре ТЗ

Новый пункт	Новая редакция
2.13	**Требования транспортабельности** Условия транспортирования составных частей МПЦ-И должны соответствовать в части воздействия: • климатических факторов − группе 5 (ОЖ4), согласно ГОСТ 15150-69; • механических нагрузок − группе Л, согласно ГОСТ 23216-78. Транспортирование МПЦ-И должно производиться в упаковке и транспортной таре всеми видами транспорта при условии соблюдения требований, установленных манипуляционными знаками, нанесёнными на транспортную тару. При транспортировании составные части МПЦ-И в транспортной таре должны быть закреплены в соответствии с действующими «Техническими условиями погрузки и крепления грузов». Испытания МПЦ-И по устойчивости к транспортной тряске должны проводиться один раз при выпуске установочной партии. Составные части МПЦ-И после воздействия механических нагрузок и климатических факторов, возникающих при их транспортировании в упаковке и транспортной таре, должны сохранять характеристики в пределах норм, установленных данным техническим заданием.
2.14	**Требования безопасности и охраны здоровья** МПЦ-И в соответствии с ГОСТ 12.1.012-2004 не должна относиться к виброопасным изделиям (во всех режимах и условиях нормального применения). Уровень излучения, создаваемый МПЦ-И должен соответствовать ГОСТ 12.1.002-84. МПЦ-И в соответствии с гигиеническим нормативом по шуму согласно ГОСТ 12.1.003-2014 не должна создавать опасный для здоровья уровень шума.
2.15	**Требования технологичности** При разработке МПЦ-И должна использоваться современная элементная база, включая микропроцессоры. Технологическая независимость МПЦ-И должна обеспечиваться последующей заменой элементов иностранного производства отечественными аналогами при их появлении на рынке электронных компонентов.
2.16	**Требования охраны окружающей среды** Применение МПЦ-И по назначению не должно оказывать вредного влияния на окружающую среду на протяжении всего жизненного цикла. Разработка МПЦ-И должна вестись с учетом ресурсосберегающих технологий.
2.17	**Требования к утилизации** Утилизация составных частей МПЦ-И должна исключать опасные и вредные влияния на окружающую среду. Утилизация МПЦ-И должна производиться в соответствии с федеральным законом от 24.06.1998 №89-ФЗ "Об отходах производства и потребления".

Новый пункт	Новая редакция
2.18	**Требования к сырью, материалам и комплектующим** Срок службы материалов, используемых при производстве МПЦ-И, должен быть не менее срока службы системы. Материалы, используемые при производстве МПЦ-И, должны соответствовать требованиям национальных стандартов и технических регламентов на поставку, транспортирование и хранение. При производстве МПЦ-И должны применяться современные комплектующие, обеспечивающие высокую надежность и правильное функционирование системы.
2.19	**Требования к консервации, упаковке и маркировке** Упаковка составных частей МПЦ-И должна обеспечивать вариант временной защиты ВЗ-10 по ГОСТ 23216-78. Упаковка составных частей МПЦ-И должна обеспечивать их защиту от влияния внешней среды и соответствовать типу ВУ-IIIА в соответствии с ГОСТ 23216-78. Составные части МПЦ-И в упаковке должны размещаться в транспортной таре, предохраняющей их от перемещения и ударов при транспортировании. Транспортная тара должна соответствовать конструкторской документации на нее и требованиям ГОСТ 23216-78 для условий транспортирования ОЖ4. Маркировка составных частей МПЦ-И должна сохранять четкость в течение назначенного срока службы устройства. Маркировка составных частей МПЦ-И должна соответствовать конструкторской документации и содержать: • наименование изготовителя и/или его товарный знак; • код изделия в соответствии с его технической документацией; • заводской номер изделия; • дату изготовления (год и месяц в соответствии с периодичностью изготовления изделия); • знак соответствия (для сертифицированных изделий).
2.20	**Требования к средствам обучения эксплуатационного персонала** Для обучения обслуживающего персонала навыкам работы с МПЦ-И должны использоваться демонстрационные стенды.

3 ЭТАПЫ ВЫПОЛНЕНИЯ ОКР

Этапы совершенствования и модернизации МПЦ-И должны соответствовать требованиям ГОСТ 33477-2015 и СТО РЖД 08.021-2015 для модели организации работ: инициативная разработка без конкретного заказчика при коммерческом риске АО "НПЦ "Промэлектроника". Этапы разработки МПЦ-И приведённые в таблице 4, должны учитывать требования «Положения о порядке проведения работ по обеспечению кибербезопасности микропроцессорных систем управления ОАО «РЖД» утверждённого Старшим вице-президентом ОАО «РЖД» В.А. Гапановичем 19.09.2014 г. N 390, а так же учитывать работы, изложенные в «Плане работ по импортозамещению и обеспечению кибербезопасности аппаратно-программных средств МПЦ-И» Утверждённого заместителем генерального директора - главным инженером ОАО «РЖД» С.А. Кобзевым от 26 августа 2019 г.

Перечень выполняемых этапов и объем документации по ним устанавливается в зависимости от степени выполняемого совершенствования или модернизации системы.

Этапы разработки программного обеспечения МПЦ-И должны соответствовать требованиям ГОСТ Р МЭК 62279-2016. Состав и содержание программной документации МПЦ-И должны выполняться в соответствии с СТО РЖД 02.051-2015.

Таблица 4 – этапы совершенствования и модернизации МПЦ-И

Этапы выполнения ОКР	**Выполняемая работа и документация**
Разработка технического задания	Техническое задание
Разработка технической документации	Техническое предложение
	Эскизный проект
	Технический проект
	Конструкторская и программная документация

	Эксплуатационная документация
	Программа обеспечения безопасности
	Доказательство безопасности
	Проект технических условий (ТУ)
Изготовление опытного образца	Изготовление
	Акт об изготовлении опытного образца
Предварительные (заводские) испытания	Программы и методики предварительных (заводских) испытаний
	Проведение испытаний
	Протоколы испытаний
	Экспертные заключения по результатам испытаний
Корректировка конструкторской и программной документации	Конструкторская и программная документация с литерой «О»
Монтаж опытного образца на объекте испытаний	Разработка проекта
	Монтажные работы
	Пуско-наладочные работы
Проведение эксплуатационных испытаний	Программа и методика эксплуатационных испытаний
	Акт приемки в опытную эксплуатацию
	Проведение испытаний
	Уведомление о готовности к приемочным испытаниям
Проведение приемочных испытаний	Программа и методика приемочных испытаний
	Проведение испытаний
	Акт приемочной комиссии
	Конструкторская документация с литерой «О1»
	Технические условия
Постановка на производство	Технологическая и программная документация
	Установочная серия
	Квалификационные испытания
	Конструкторская документация с литерой «А»
Декларирование	По плану проекта

4 ПОРЯДОК ВЫПОЛНЕНИЯ И ПРИЁМКИ ЭТАПОВ ОКР

Порядок выполнения и приемки ОКР по совершенствованию и модернизации МПЦ-И должен соответствовать требованиям ГОСТ 33477-2015 и СТО РЖД 08.021-2015 для модели организации работ: инициативная разработка без конкретного заказчика при коммерческом риске АО "НПЦ "Промэлектроника". Порядок выполнения и приемки приведен в таблице 5.

Таблица 5 – порядок выполнения и приёмки

Этапы выполнения ОКР	**Работы и разрабатываемая документация**	**Приемка ОКР**		
		ОАО «РЖД»	**АО «НПЦ «Промэлектроника»**	**Испытательный центр/Экспертная организация**
Разработка технического задания	Техническое задание (по ГОСТ 33477)	Согласование	Разработка, утверждение	Согласование ИЦ СЦБ«Эксперт»
Разработка технической документации	Техническое предложение (по ГОСТ 2.118)	-	Разработка, согласование, утверждение	-
	Эскизный проект (по ГОСТ 2.119)	-	Разработка, согласование, утверждение	
	Технический проект (по ГОСТ 2.120)	-	Разработка, согласование, утверждение	-
	Конструкторская и программная документация (по ЕСКД и ЕСПД)	-	Разработка, согласование, утверждение	-
	Эксплуатационная документация (по ГОСТ 2.601)	Согласование	Разработка, утверждение	-
	Программа обеспечения безопасности (по ГОСТ 33432)	Согласование	Разработка, утверждение	Экспертное заключение ИЦ СЦБ«Эксперт»
	Доказательство безопасности (по ГОСТ 33432)	Согласование	Разработка, утверждение	Экспертное заключение ИЦ СЦБ«Эксперт»
	Проект технических условий (ТУ)		Разработка	-

Этапы выполнения ОКР	**Работы и разрабатываемая документация**	**Приемка ОКР**		
		ОАО «РЖД»	**АО «НПЦ «Промэлектроника»**	**Испытательный центр/Экспертная организация**
Изготовление опытного образца	Акт об изготовлении опытного образца (по ГОСТ 33477)	-	Подписание	-
Предварительные (заводские) испытания	Программы и методики предварительных (заводских) испытаний (по ГОСТ 2.106-9)	-	Разработка, Утверждение	Согласование ИЦ СЦБ«Эксперт»
	Проведение испытаний	-	Организация, Проведение	Участие ИЦ СЦБ«Эксперт»
	Протоколы испытаний, экспертные Заключения	-	Согласование Утверждение	Экспертные Заключения ИЦ СЦБ«Эксперт»
Испытания на кибербезопасность модернизированного варианта на базе защищённой доверенной среды загрузки (защищённый вариант БИОС)	Протоколы испытаний, экспертные заключения	-	-	Участие Экспертное заключение АО «НИИАС»
Корректировка КД и ПД	Конструкторская и программная документация с литерой «О» (по ЕКСД и ЕСПД)	-	Корректировка, согласование	-

Этапы выполнения ОКР	**Работы и разрабатываемая документация**	**Приемка ОКР**		
		ОАО «РЖД»	**АО «НПЦ «Промэлектроника»**	**Испытательный центр /Экспертная организация**
Монтаж опытного образца на объекте испытаний	Разработка технического решения (ТР) (по СП 235.1326000.2015)	Утверждение	Разработка, согласование	-
	Разработка проекта (РП) (по СП 235.1326000.2015 и техническим решениям)			
	Монтажные работы Пусконаладочные работы (по инструкции по монтажу и рабочему проекту)	Выбор объекта	Пуско-наладка	-
Проведение эксплуатационных испытаний	Программа и методика эксплуатационных испытаний (по ГОСТ 2.106)	Утверждение	Разработка, согласование	Согласование ИЦ СЦБ«Эксперт»
	Акт приемки в опытную эксплуатацию	Утверждение	Согласование	Согласование ИЦ СЦБ«Эксперт»

Этапы выполнения ОКР	**Работы и разрабатываемая документация**	**Приемка ОКР**		
		ОАО «РЖД»	**АО «НПЦ «Промэлектроника»**	**Испытательный центр /Экспертная организация**
Проведение приемочных испытаний	Программа и методика приемочных испытаний (по ГОСТ 2.106)	Утверждение	Разработка, согласование	Согласование ИЦ СЦБ«Эксперт»
	Проведение испытаний (на объекте ОАО «РЖД»)	Участие	Проведение Организация	Участие ИЦ СЦБ«Эксперт»
	Акт приемочной комиссии (по ГОСТ 33477)	Утверждение	Согласование	Согласование ИЦ СЦБ«Эксперт»
	Конструкторская документация с литерой «О1» (по ЕСКД), ТУ	Согласование	Разработка Согласование Утверждение	-
Постановка на производство	Технологическая и программная документация (по ЕСТД и ЕСПД)	-	Разработка Согласование Утверждение	-
	Установочная серия	-	Изготовление, авторский надзор	-
	Программа и методика квалификационных испытаний	-	Разработка, согласование, утверждение	-
	Квалификационные испытания	-	Проведение	-
	Конструкторская документация с литерой «А» (по ЕСКД)	-	Согласование	-

Этапы выполнения ОКР	**Работы и разрабатываемая документация**	**Приемка ОКР**		
		ОАО «РЖД»	**АО «НПЦ «Промэлектроника»**	**Испытательный центр /Экспертная организация**
Проведение подконтрольной эксплуатации (по решению приемочной комиссии)	Программа и методика подконтрольной эксплуатации	Утверждение	Разработка	Согласование ИЦ СЦБ«Эксперт»
	Проведение	Организация	Участие Контроль	Участие ИЦ СЦБ«Эксперт»
	Акт о завершении	Утверждение	Подписание	Согласование ИЦ СЦБ«Эксперт»
Подтверждение соответствия	Работы по подтверждению соответствия	-	Организация Участие	Проведение Оформление заключения ИЦ СЦБ«Эксперт»
Допуск продукции к применению	Перечень систем, аппаратуры и оборудования ЖД автоматики и телемеханики, разрешенных по результатам приемочных испытаний к применению (проектированию) для объектов ОАО «РЖД»	Утверждение	-	-

ПРИЛОЖЕНИЕ А

(справочное)

Перечень ссылочных нормативных документов

ГОСТ 2.106-96 Единая система конструкторской документации (ЕСКД). Текстовые документы

ГОСТ 2.118-2013 Единая система конструкторской документации. Техническое предложение

ГОСТ 2.119-2013 Единая система конструкторской документации. Эскизный проект

ГОСТ 2.120-2013 Единая система конструкторской документации. Технический проект

ГОСТ 2.601-2013 Единая система конструкторской документации. Эксплуатационные документы

ГОСТ 12.1.002-84 Система стандартов безопасности труда. Электрические поля промышленной частоты. Допустимые уровни напряженности и требования к проведению контроля на рабочих местах

ГОСТ 12.1.003-2014 Система стандартов безопасности труда. Шум. Общие требования безопасности

ГОСТ 12.2.007.0-75 Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности

ГОСТ 12.1.012-2004 Система стандартов безопасности труда. Вибрационная безопасность. Общие требования

ГОСТ 15150-69 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды

ГОСТ 21889-76 Система "Человек-машина". Кресло человека-оператора. Общие эргономические требования

ГОСТ 22269-76 Система "Человек-машина". Рабочее место оператора. взаимное расположение элементов рабочего места. Общие эргономические требования

ГОСТ 23000-76 Система "Человек-машина". Пульты управления. Общие эргономические требования

ГОСТ 23216-78 Изделия электротехнические. Хранение, транспортирование, временная противокоррозионная защита, упаковка. Общие требования и методы испытаний

ГОСТ 24.701-86 Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения

ГОСТ 24750-81 Средства технические вычислительной техники. Общие требования технической эстетики

ГОСТ 25861-83 Машины вычислительные и системы обработки данных. Требования электрической и механической безопасности и методы испытаний

ГОСТ 27.301-83 Надежность в технике. Прогнозирование надежности изделий при проектировании. Общие требования

ГОСТ Р 27.403-2009 Надежность в технике. Планы испытаний для контроля вероятности безотказной работы

ГОСТ 27.003-2016 Надежность в технике (ССНТ). Состав и общие правила задания требований по надежности

ГОСТ 30804.6.4-2013 Совместимость технических средств электромагнитная. Электромагнитные помехи от технических средств, применяемых в промышленных зонах. Нормы и методы испытаний

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

ГОСТ 33436.4-1-2015 Совместимость технических средств электромагнитная. Системы и оборудование железнодорожного транспорта. Часть 4-1. Устройства и аппаратура железнодорожной автоматики и телемеханики. Требования и методы испытаний

ГОСТ 33477-2015 Система разработки и постановки продукции на производство (СРПП). Технические средства железнодорожной инфраструктуры. Порядок разработки, постановки на производство и допуска к применению

ГОСТ 33894-2016 Система железнодорожной автоматики и телемеханики на железнодорожных станциях. Требования безопасности и методы контроля

ГОСТ 34012-2016 Аппаратура железнодорожной автоматики и телемеханики. Общие технические требования

ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ Р 50923-96 Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения

ГОСТ Р 50933-96 Каналы и тракты внутризоновых радиорелейных линий. Основные параметры и методы измерений

ГОСТ Р 50948-2001 Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности

ГОСТ Р 51341-99 Эргономические требования по конструированию средств отображения информации и органов управления. Часть 2. Средства отображения информации

ГОСТ Р 52980-2008 Системы промышленной автоматизации и их интеграция. Системы программируемые электронные железнодорожного применения. Требования к программному обеспечению

ГОСТ Р МЭК 61508-1-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

ГОСТ Р МЭК 61508-2-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам

ГОСТ Р МЭК 61508-3-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

ГОСТ Р МЭК 61508-7-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства

ГОСТ Р МЭК 62279-2016 Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах

ГОСТ Р ИСО/МЭК 9126-93 Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению

СТО РЖД 02.049-2014 Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия

СТО РЖД 08.021 Устройство железнодорожной автоматики и телемеханики. Порядок разработки, испытаний и постановки на производство

СТО РЖД 08.051—2015 Микропроцессорные устройства железнодорожной автоматики и телемеханики. Программное обеспечение. Требования функциональной безопасности

СТО РЖД 1.19.004-2008 Автоматизированные системы управления движением поездов на станциях. Общие технические требования

СТО РЖД 1.19.005-2008 Системы и устройства железнодорожной автоматики и телемеханики. Условные графические изображения

Правила технической эксплуатации железных дорог Российской Федерации, утв. приказом Минтранса России от 21.12.2010 г. № 286;

Инструкция по сигнализации на железнодорожном транспорте Российской Федерации (Приложение №7 к ПТЭ), введена приказом Минтранса России от 04.06.2012 г. № 162;

Инструкция по движению поездов и маневровой работе на железнодорожном транспорте Российской Федерации (Приложение №8 к ПТЭ), введена приказом Минтранса России от 04.06.2012 г. № 162;

Инструкция по техническому обслуживанию и ремонту устройств и систем СЦБ от 30.12.2015 г. №3168р

Свод правил СП 235.1326000.2015 "Железнодорожная автоматика и телемеханика. Правила проектирования", утв. приказом Минтранса России от 06.07.2015 г. № 205.

Технический регламент Таможенного союза ТР ТС 003/2011 «О безопасности инфраструктуры железнодорожного транспорта»

Федеральный закон от 24.06.1998 № 89-ФЗ «Об отходах производства и потребления»

СанПиН 2.2.2/2.4.1340-03 Санитарные нормы и правила. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы

Приказ ФСТЭК России от 14 марта 2014 г. №31 «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Положение о порядке проведения работ по обеспечению кибербезопасности микропроцессорных систем управления ОАО «РЖД » утверждённого Старшим вице-президентом ОАО «РЖД » В.А. Гапановичем 19.09.2014 г

Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» от 30 марта 1992 г.

Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» от 25 июля 1997 г.

D.S432359-00205 МПЦ-И. Обеспечение горячего резервирования УКЦ. Технические требования