ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 54957— 2012

ЖЕЛЕЗНОДОРОЖНАЯ ЭЛЕКТРОСВЯЗЬ

Общие требования безопасности

Издание официальное

Москва
Стандартинформ
2013

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «ТрансТелеКом-Бизнес» (ООО «ТрансТелеКом-Бизнес»)

2 ВНЕСЕН техническим комитетом по стандартизации ТК 45 «Железнодорожный транспорт»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 16 августа 2012 г. № 242-ст

4 Настоящий стандарт может быть применен на добровольной основе для соблюдения требований технических регламентов Таможенного союза:
«О безопасности инфраструктуры железнодорожного транспорта»;
«О безопасности высокоскоростного железнодорожного транспорта»

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

Содержание

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЖЕЛЕЗНОДОРОЖНАЯ ЭЛЕКТРОСВЯЗЬ

Общие требования безопасности

Railway telecommunications.
General safety requirements

Дата введения — 2012—09—01

1 Область применения

Настоящий стандарт распространяется на средства, системы, сети и ресурсы железнодорожной электросвязи и устанавливает общие требования безопасности в области железнодорожной электросвязи.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК ТО 13335-1—2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

ГОСТ Р ИСО/МЭК 13335-5—2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

ГОСТ Р ИСО/МЭК ТО 15271—2002 Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)

ГОСТ Р ИСО/МЭК 15408-1—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК 17799—2005 Информационная технология. Практические правила управления информационной безопасностью

ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р 50648—94 (МЭК 1000-4-8—93) Совместимость технических средств электромагнитная. Устойчивость к магнитному полю промышленной частоты. Технические требования и методы испытаний

ГОСТ Р 50922—2006 Защита информации. Основные термины и определения

ГОСТ Р 51275—2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 51317.4.2—2010 (МЭК 61000-4-2:2008) Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Требования и методы испытаний

Издание официальное

ГОСТ Р 51317.4.3—2006 (МЭК 61000-4-3:2006) Совместимость технических средств электромагнитная. Устойчивость к радиочастотному электромагнитному полю. Требования и методы испытаний

ГОСТ Р 51317.4.4—2007 (МЭК 61000-4-4:2004) Совместимость технических средств электромагнитная. Устойчивость к наносекундным импульсным помехам. Требования и методы испытаний

ГОСТ Р 51317.4.5—99 (МЭК 61000-4-5—95) Совместимость технических средств электромагнитная. Устойчивость к микросекундным импульсным помехам большой энергии. Требования и методы испытаний

ГОСТ Р 51317.4.6—99 (МЭК 61000-4-6—96) Совместимость технических средств электромагнитная. Устойчивость к кондуктивным помехам, наведенным радиочастотными электромагнитными полями. Требования и методы испытаний

ГОСТ Р 51317.4.11—2007 (МЭК 61000-4-11:2004) Совместимость технических средств электромагнитная. Устойчивость к провалам, кратковременным прерываниям и изменениям напряжения электропитания. Требования и методы испытаний

ГОСТ Р 51317.4.16-2000 (МЭК 61000-4-16—98) Совместимость технических средств электромагнитная. Устойчивость к кондуктивным помехам в полосе частот от 0 до 150 кГц. Требования и методы испытаний

ГОСТ Р 52448—2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения

ГОСТ Р 53953—2010 Электросвязь железнодорожная. Термины и определения

ГОСТ Р МЭК 61508 (все части)—2007 Функциональная безопасность электрических, электронных, программируемых электронных систем, связанных с безопасностью

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р МЭК 61508-4, ГОСТ Р 52448, ГОСТ Р ИСО МЭК 15408-1, ГОСТ Р 50922, ГОСТ Р 53953, а также следующие термины с соответствующими определениями:

3.1 **безопасность инфраструктуры железнодорожного транспорта:** Состояние инфраструктуры железнодорожного транспорта в целом, определяемое через состояние его подсистем и их взаимодействие между собой и железнодорожным подвижным составом, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу; окружающей среде, жизни или здоровью животных и растений.

3.2 **железнодорожная линия:** Технологический комплекс, включающий в себя железнодорожные пути и железнодорожные станции с полосой отвода и совокупность (полную или частично) устройств железнодорожного электроснабжения, железнодорожной автоматики и телемеханики, железнодорожной электросвязи и иные, обеспечивающие функционирование этого комплекса, здания, строения, сооружения, устройства и оборудование.

3.3

сбой: Самоустраняющийся отказ или однократный отказ, устранимый незначительным вмешательством оператора.

[ГОСТ Р ИСО/МЭК 27001—2006, пункт 3.13]

3.4 **требования безопасности:** Требования, установленные законодательными актами, нормативно-техническими и проектными документами, правилами и инструкциями, выполнение которых обеспечивает безопасные условия функционирования сети железнодорожной электросвязи.

3.5 **элементы функциональных подсистем:** Изделия и конструкции, применяемые при строительстве и монтаже составных частей функциональных подсистем.

4 Общие положения

4.1 Цели обеспечения безопасности железнодорожной электросвязи

Основными целями обеспечения безопасности железнодорожной электросвязи являются:

- достижение устойчивого функционирования и успешного выполнения заданных функций средствами, системами, сетями железнодорожной электросвязи в условиях возможного воздействия нарушителя, способного привести к нарушению конфиденциальности, целостности, доступности или подотчетности;

- обеспечение доступности услуг связи, особенно услуг экстренного обслуживания в чрезвычайных ситуациях, в том числе и в случае террористических актов.

4.2 Основные задачи обеспечения безопасности железнодорожной электросвязи

Основными задачами обеспечения безопасности железнодорожной электросвязи являются:

- своевременное выявление, оценка и прогнозирование источников угроз безопасности, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития систем и сетей железнодорожной электросвязи;

- выявление и устранение уязвимостей в средствах, системах и сетях железнодорожной электросвязи;

- предотвращение, обнаружение угроз безопасности, пресечение их реализации и своевременная ликвидация последствий возможных воздействий нарушителя, в том числе и террористических действий;

- совершенствование применяемых мер обеспечения безопасности железнодорожной электросвязи.

4.3 Средства, сети, системы и виды железнодорожной электросвязи

4.3.1 К железнодорожной электросвязи относятся:

- средства связи, выполняющие функции систем коммутации;
- средства связи, выполняющие функции цифровых транспортных систем;
- средства связи, выполняющие функции систем управления и мониторинга;
- оборудование, используемое для учета объема оказанных услуг связи в сетях связи общего пользования;
- оборудование средств связи, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий;
- радиоэлектронные средства связи;
- оконечное оборудование;
- кабели связи и линейно-кабельные сооружения связи;
- антенны и фидерные устройства;
- оборудование, реализующее дополнительные сетевые услуги;
- оборудование электропитания средств связи.

4.3.2 К сетям железнодорожной электросвязи относятся:

- первичная сеть связи железнодорожного транспорта;
- вторичные сети железнодорожной электросвязи:
  - а) сеть оперативно-технологической связи;
  - б) сеть общетехнологической телефонной связи;
  - в) железнодорожная телеграфная сеть;
  - г) сеть передачи данных оперативно-технологического назначения;
  - д) сеть передачи данных общетехнологического назначения;
  - ж) сеть автоматизированной документальной связи;
  - и) сеть железнодорожной радиосвязи;
  - к) сеть технологической спутниковой связи.

4.3.3 К системам, предназначенным для построения указанных сетей железнодорожной электросвязи, относятся:

- волоконно-оптическая система передачи;
- система передачи по кабелю с медными жилами;
- радиорелейная система передачи;
- спутниковая система передачи;
- система технологической аудиоконференцсвязи;

- система технологической видеоконференцсвязи;
- система документированной регистрации служебных переговоров;
- система железнодорожной радиосвязи;
- система поездной радиосвязи;
- система станционной радиосвязи;
- система ремонтно-оперативной радиосвязи;
- система передачи данных по радиоканалу;
- транкинговая система технологической радиосвязи;
- система мониторинга и администрирования сетью железнодорожной электросвязи;
- система тактовой сетевой синхронизации цифровой сети железнодорожной электросвязи;
- система оперативно-розыскных мероприятий и др.

4.3.4 Существуют следующие виды железнодорожной электросвязи:

- поездная диспетчерская;
- поездная межстанционная;
- постанционная;
- линейно-путевая;
- стрелочная;
- энергодиспетчерская;
- перегонная;
- служебная связь электромехаников сигнализации, централизации, блокировки и связи;
- магистральная;
- дорожная;
- дорожная распорядительная;
- билетно-диспетчерская;
- вагонно-диспетчерская;
- маневровая диспетчерская;
- местная;
- двухсторонняя парковая;
- оповещения пассажиров.

4.4 Основные уязвимости, угрозы

4.4.1 При определении уязвимостей различают объективные, субъективные и случайные:

- объективными являются уязвимости, зависящие от особенностей построения и технических характеристик. Полное устранение данных уязвимостей невозможно, тем не менее они могут существенно ослабляться техническими и инженерно-техническими методами;

- субъективными являются уязвимости, зависящие от действий сотрудников, которые устраняются в большей части организационными и программно-аппаратными методами;

- случайными являются уязвимости, зависящие от особенностей окружающей среды и непредвиденных обстоятельств.

4.4.2 Угрозой безопасности функционирования средств, систем и сетей железнодорожной электросвязи является совокупность условий и факторов, создающих потенциальную или реальную опасность несанкционированных и (или) непреднамеренных воздействий на информационные ресурсы и телекоммуникационную составляющую железнодорожной электросвязи, что может привести к нарушению выполняемых ими функций, риску нанесения им ущерба и возникновению чрезвычайных ситуаций.

4.4.2.1 Для разработки и осуществления планов обеспечения безопасности должны быть определены: комбинация угроз, уязвимостей, воздействий нарушителя и оценка защищаемых систем и ресурсов, чтобы выработать решения по устранению или уменьшению угроз, устранению или ослаблению уязвимости и координации управления риском.

4.4.2.2 Каждая выявленная угроза должна быть описана и включена в перечень угроз безопасности. Рекомендуемый перечень основных угроз и включенные в него угрозы безопасности приведены в приложении А.

4.4.2.3 Угрозы безопасности в соответствии с архитектурой безопасности согласно [1] могут быть отнесены к техническим средствам сети электросвязи и (или) пользователей в соответствии с таблицей 4.1.

Таблица 4.1

Краткое наименование угрозы	Описание угрозы	Применимость	
		к техническим средствам сети электросвязи	к техническим средствам пользователей
Уничтожение	Разрушение информации и (или) других ресурсов	+	+
Искажение	Искажение или изменение информации	+	+
Утечка	Удаление, кража или потеря информации и (или) других ресурсов	+	+
Разглашение	Раскрытие информации	+	+
Блокирование	Прерывание обслуживания	+	–
Примечание — Применимость угроз к техническим средствам сети электросвязи и техническим средствам пользователей должны определяться политикой информационной безопасности.			

4.4.2.4 При классификации объектов, на которые направлены угрозы, применяют три уровня:
- инфраструктура сети,
- услуги связи,
- приложения.

Уровень инфраструктуры сети охватывает информацию пользователей, уровень услуг связи — услуги сети, уровень приложений — приложения, организуемые на базе сетей связи.

4.4.2.5 Угрозы разделяют на преднамеренные и непреднамеренные, активные и пассивные. Пассивная угроза — угроза несанкционированного раскрытия информации без изменения состояния автоматизированной системы. К активным относят угрозы, которые вызывают изменения информации, содержащейся в системе, а также изменения состояния или работы этой системы.

4.4.2.6 К угрозам информационной безопасности относят:
- нарушение целостности информации;
- модификация сообщения;
- отказ отправителя (получателя) от факта отправления (получения) информации;
- отказ в обслуживании;
- вирусы;
- спам;
- слежка;
- закладки в оборудование и программное обеспечение;
- злоупотребление доверием;
- переадресация портов;
- вставка фальшивого трафика;
- искажение данных систем управления, маршрутизации и др.

4.5 Критерии оценки безопасности

4.5.1 В таблице 4.2 установлена взаимосвязь основных угроз и критериев безопасности сети электросвязи.

Таблица 4.2

Вид угрозы	Критерии безопасности			
	Конфиденциальность	Целостность	Доступность	Подотчетность
Уничтожение информации и (или) других ресурсов	–	+	+	+
Искажение или модификация информации	–	+	–	+
Мошенничество	+	+	+	+
Кража, утечка, потеря информации и (или) других ресурсов	+	+	+	–

Окончание таблицы 4.2

Вид угрозы	Критерии безопасности			
	Конфиденциальность	Целостность	Доступность	Подотчетность
Несанкционированный доступ	+	+	+	+
Отказ в обслуживании	–	–	+	–
Примечание — Знак «+» означает возможное воздействие угрозы на критерий безопасности, знак «–» — отсутствие угрозы критерию безопасности.				

4.5.2 Нарушение конфиденциальности, целостности, доступности или подотчетности при потенциальном воздействии нарушителя может иметь следующие последствия для деятельности оператора связи и состояния инфокоммуникационной структуры сети электросвязи:

- «низкое» потенциальное воздействие может привести к ограниченному неблагоприятному эффекту, т. е. ситуации в подсистеме железнодорожной электросвязи, при которой нанесенный ущерб является восполнимым или восстановимым в короткий срок;
- «умеренное» потенциальное воздействие может привести к серьезному неблагоприятному эффекту, т. е. ситуации в подсистеме железнодорожной электросвязи, при которой нанесенный ущерб является восполнимым в средние или долгие сроки;
- «высокое» потенциальное воздействие может привести к тяжелому или катастрофическому неблагоприятному эффекту, т. е. особой ситуации в подсистеме железнодорожной электросвязи, при возникновении которой предотвращение гибели людей оказывается невозможным.

4.6 Уровни обеспечения безопасности

Архитектуру безопасности согласно [1, 2] определяют два основных понятия:

- уровень;
- плоскость.

Понятие уровня архитектуры безопасности используется при формировании требований к средствам, системам и сетям, образующим подсистему железнодорожной электросвязи.

В таблице 4.3 приведены три уровня безопасности согласно [1], а также их применимость к техническим средствам сети железнодорожной электросвязи и к техническим средствам пользователей.

Таблица 4.3

Уровни безопасности	Применимость	
	к техническим средствам сети электросвязи	к техническим средствам пользователей
Уровень безопасности инфраструктуры	+	–
Уровень безопасности услуг	+	+
Уровень безопасности приложений	+	+

4.7 Плоскости обеспечения безопасности

Архитектура безопасности в части защиты сетевых операций использует понятие плоскостей согласно [1—5]. Архитектура безопасности определяет три плоскости, соответствующие трем видам операций, осуществляемых в подсистеме железнодорожной электросвязи. Плоскостями обеспечения безопасности являются:

- плоскость административного управления согласно [2];
- плоскость оперативного управления (соответствует уровню доступа к услугам и ресурсам сети) согласно [1];
- плоскость конечного пользователя (соответствует уровню клиентского оборудования) согласно [1].

В таблице 4.4 приведены три плоскости обеспечения безопасности, а также их применимость к сети железнодорожной электросвязи и к техническим средствам пользователей.

Таблица 4.4

Плоскости обеспечения безопасности	Применимость	
	к техническим средствам сети электросвязи	к техническим средствам пользователей
Плоскость административного управления	+	+*
Плоскость оперативного управления	+	+
Плоскость конечного пользователя	+	+
* Отсутствует в случаях, когда пользователь не использует управление сетью/службой.		

4.8 Для определения требований к обеспечению безопасности средств, систем и сетей железнодорожной электросвязи необходимо определение модели угроз согласно ГОСТ Р 52448 (приложение А).

4.9 Для снижения рисков должны быть реализованы требования к средствам управления согласно ГОСТ Р ИСО/МЭК 27001 и должны быть выполнены общие мероприятия по управлению информационной безопасностью согласно ГОСТ Р ИСО/МЭК 17799.

4.10 При выборе обобщенных критериев оценки безопасности железнодорожной электросвязи необходимо учитывать оценки безопасности на каждом из уровней (инфраструктуры, транспорта/передачи и функционального, приложений).

4.10.1 Уровень инфраструктуры

4.10.1.1 Средства и системы инфраструктуры железнодорожной электросвязи, подлежащие защите:

- линии связи;
- направляющие линии поездной радиосвязи (направляющие системы).

4.10.1.2 Классификация факторов, воздействующих на инфраструктуру

Перечень объективных факторов, воздействующих на инфраструктуру железнодорожной электросвязи:

а) внутренние факторы:

1) старение материалов (металла, резины);

б) внешние факторы:

1) факторы техногенного характера;

2) природные явления, стихийные бедствия.

Перечень субъективных факторов, воздействующих на инфраструктуру железнодорожной электросвязи:

а) внутренние факторы:

1) неправомерные действия лиц, имеющих право доступа к линиям связи и направляющим системам:

- несанкционированное изменение инфраструктуры железнодорожной электросвязи;

б) несанкционированный физический доступ к линиям связи и направляющим системам:

1) хищение линий связи и направляющих систем;

2) действия, направленные на изменение инфраструктуры железнодорожной электросвязи.

4.10.1.3 Уязвимостями инфраструктуры железнодорожной электросвязи являются:

а) объективные:

1) активизируемые — аппаратные закладки (устанавливаемые в линии электросвязи, сети электропитания, в помещениях);

2) определяемые особенностями элементов — элементы, подверженные воздействию окружающей среды (дождь, снег, солнце, другие климатические факторы);

3) определяемые особенностями защищаемого объекта — местоположением объекта (отсутствие контролируемой зоны, наличие прямой видимости объектов, удаленных и подвижных элементов объекта);

б) субъективные:

1) ошибки: при установке или эксплуатации объектов инфраструктуры железнодорожной электросвязи;

2) нарушения: режима охраны и защиты (доступа на объект, доступа к техническим средствам); режима эксплуатации технических средств (энергообеспечения, жизнеобеспечения); режима

использования информации (обработка и обмен информацией, хранение и уничтожение носителей информации, уничтожения производственных отходов и брака); режима конфиденциальности.

в) случайные:

1) сбои и отказы: старение элементов инфраструктуры железнодорожной электросвязи; сбои электроснабжения (вспомогательного оборудования);

2) повреждения: жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации; кондиционирования и вентиляции); ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий; корпусов технологического оборудования).

4.10.1.4 Источниками дестабилизирующих воздействий на инфраструктуру железнодорожной электросвязи являются:

а) источники, обусловленные действиями субъекта:

1) внешние источники:

- случайные (непреднамеренные) — персонал поставщиков различного рода услуг, персонал надзорных организаций и аварийных служб и др.;
- преднамеренные — потенциальные преступники (террористы) и хакеры; недобросовестные партнеры; представители силовых структур (в чрезвычайных ситуациях);

2) внутренние источники: основной персонал; представители служб безопасности; обслуживающий персонал; технический персонал (жизнеобеспечение, эксплуатация). Внутренние источники могут использовать каждый из классов уязвимостей (объективные, субъективные, случайные) в зависимости от преследуемых целей. Угрозы от данных источников могут быть: хищение; уничтожение; нарушение доступности (блокирование);

б) источники, обусловленные действиями материального объекта:

1) внешние источники: сети инженерных коммуникаций (водоснабжение, канализация);

2) внутренние источники: средства охраны сигнализации.

в) физические явления: пожары, землетрясения, ураганы, наводнения и др.

4.10.1.5 Возможна реализация любых угроз см. ГОСТ Р 52448. Возможные последствия реализации угроз — нарушение любого из критериев безопасности сети электросвязи (конфиденциальность, целостность, доступность, подотчетность).

4.10.1.6 Возникновение уязвимостей на уровне инфраструктуры железнодорожной электросвязи возможно на стадиях их жизненного цикла.

4.10.1.7 Критерии оценки безопасности инфраструктуры железнодорожной электросвязи:

- на стадии планирования: соответствие требованиям безопасности в части линий связи и направляющих систем, предъявляемых стратегическими целями железнодорожной электросвязи;
- на стадии проектирования: соответствие характеристик проектируемых линий связи и направляющих систем требованиям безопасности, предъявляемым на стадии планирования;
- на стадии эксплуатации и строительства: соответствие линий связи и направляющих систем заявленным поставщиком характеристикам;
- на стадии вывода из эксплуатации: соответствие требованиям безопасности по выводу из эксплуатации линий связи и направляющих систем.

4.10.2 Уровень транспорта/передачи и функциональный уровень

4.10.2.1 Средства и системы передачи информации железнодорожной электросвязи, подлежащие защите:

- каналы и тракты систем передачи;
- каналообразующее оборудование;
- аппаратура передачи данных;
- аналоговые и цифровые многоканальные системы передачи;
- коммутационное оборудование;
- маршрутизаторы;
- другое оборудование первичной сети связи технологического сегмента железнодорожной электросвязи в соответствии с 4.3.

4.10.2.2 К функциональному уровню железнодорожной электросвязи относятся средства, системы, сети и ресурсы вторичных сетей связи технологического сегмента железнодорожной электросвязи.

4.10.2.3 Опасности и модели угроз безопасности средств, систем, сетей железнодорожной электросвязи на уровне транспорта/передачи и функциональном уровне

4.10.2.3.1 Опасностями являются соответствующие факторы согласно ГОСТ Р 51275.

4.10.2.3.2 Уязвимостями средств, систем, сетей железнодорожной электросвязи являются:

а) объективные:

1) сопутствующие техническим средствам излучения: электромагнитные (побочные излучения элементов технических средств, кабельных линий технических средств); электрические (наводки электромагнитных излучений на линии и проводки, просачивание сигналов в сети электропитания, в цепи заземления, неравномерность потребления тока электропитания); звуковые (акустические, виброакустические);

2) активизируемые: аппаратные закладки (устанавливаемые в линии электросвязи, в сети электропитания, в помещениях); программные закладки (вредоносные программы, технологические выходы из программ, нелегальные копии программного обеспечения);

3) определяемые особенностями элементов: элементы подверженные воздействию электромагнитного поля (магнитные носители, микросхемы);

4) определяемые особенностями защищаемого объекта: местоположением объекта (отсутствие контролируемой зоны, наличие прямой видимости объектов, наличие удаленных и подвижных элементов объекта); организацией каналов обмена информацией (использование радиоканалов, глобальных инфокоммуникационных сетей, арендуемых каналов);

б) субъективные:

1) ошибки: при подготовке и использовании программного обеспечения (инсталляция и загрузка программного обеспечения, эксплуатация программного обеспечения, ввод данных); при управлении сложными системами (организация управления потоками обмена информации); при установке или эксплуатации технических средств;

2) нарушения: режима охраны и защиты (доступ на объект, доступ к техническим средствам); режима эксплуатации технических средств (энергообеспечение, жизнеобеспечение); режима использования информации (обработка и обмен информацией, хранение и уничтожение носителей информации); режима конфиденциальности;

в) случайные:

1) сбои и отказы: отказы и неисправности технических средств (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа); старение и размагничивание носителей информации (дискет и съемных носителей, жестких дисков, микросхем); сбои программного обеспечения; сбои электроснабжения;

2) повреждения: жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации; кондиционирования и вентиляции); ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий; корпусов технологического оборудования).

4.10.2.3.3 Источники дестабилизирующих воздействий

Источники, обусловленные действиями субъекта:

а) внешние источники:

1) случайные (непреднамеренные): персонал поставщиков услуг различного рода, персонал надзорных организаций и аварийных служб и др;

2) преднамеренные: потенциальные преступники (террористы) и хакеры; недобросовестные партнеры; представители силовых структур (в чрезвычайных ситуациях) и др.;

б) внутренние источники: основной персонал; представители служб безопасности; обслуживающий персонал; технический персонал.

Источники, обусловленные действиями материального объекта:

а) внешние источники: средства связи (телефонные линии); сети инженерных коммуникаций;

б) внутренние источники: технические средства обработки информации; программные средства обработки информации; средства охраны.

Физические явления: пожары, землетрясения, ураганы, наводнения и др.

4.10.2.3.4 На рассматриваемых уровнях железнодорожной электросвязи возможна реализация любых угроз согласно 4.4. Возможными последствиями реализации угроз может быть нарушение любого из критериев безопасности сети электросвязи (конфиденциальность, целостность, доступность, подотчетность).

4.10.2.3.5 Возникновение уязвимостей на уровне инфраструктуры и линий железнодорожной электросвязи возможно на всех стадиях их жизненного цикла.

4.10.2.3.6 Реализация угроз, обусловленная действиями субъекта, характеристиками материальных объектов, физическими явлениями, возможна на стадии планирования, проектирования, строительства, эксплуатации, а также вывода из эксплуатации.

4.10.2.4 Критериями оценки безопасности средств, систем, сетей железнодорожной электросвязи на уровне транспорта/передачи и функциональном уровне являются:

- на стадии планирования: соответствие требованиям безопасности, предъявляемым стратегическими целями железнодорожной электросвязи;

- на стадии проектирования: соответствие характеристик проектируемых средств, систем, сетей железнодорожной электросвязи транспортного уровня требованиям безопасности, предъявляемых на стадии планирования;

- на стадии эксплуатации и внедрения: соответствие заявленным поставщиком характеристикам;

- на стадии вывода из эксплуатации: соответствие требованиям безопасности по выводу из эксплуатации.

4.10.3 Уровень приложений, услуг и управления

4.10.3.1 Средства и системы железнодорожной электросвязи уровня приложений, услуг и управления, подлежащие защите:

- средства территориально-распределенной иерархической автоматизированной системы управления технологической сетью связи;

- системы территориально-распределенной иерархической автоматизированной системы управления технологической сетью связи в составе:

а) системы мониторинга и администрирования, предназначенной для мониторинга параметров функционирования и интегрированного управления технологической сетью связи в целом;

б) систем управления и мониторинга производителя для обеспечения управления и технического обслуживания оборудования железнодорожной электросвязи, входящего в состав технологической сети связи железнодорожного транспорта, реализующего функциональные возможности в соответствии с уровнем управления элементом или сетью, согласно архитектуре построения сети управления железнодорожной электросвязью.

4.10.3.2 Опасности и модели угроз безопасности средств, систем и ресурсов железнодорожной электросвязи уровня приложений, услуг и управления

4.10.3.2.1 Опасностями на уровне приложений, услуг и управления являются соответствующие факторы согласно ГОСТ Р 51275.

4.10.3.2.2 Уязвимостями средств, систем и ресурсов железнодорожной электросвязи уровня приложений, услуг и управления являются:

а) объективные:

1) сопутствующие техническим средствам излучения: электромагнитные (побочные излучения элементов технических средств, кабельных линий технических средств); электрические (наводки электромагнитных излучений на линии и проводки, просачивание сигналов в сети электропитания, цепи заземления, неравномерность потребления тока электропитания); звуковые (акустические, виброакустические);

2) активизируемые: аппаратные закладки (устанавливаемые в линии электросвязи, в сети электропитания, в помещениях); программные закладки (вредоносные программы, технологические выходы из программ, нелегальные копии программного обеспечения);

3) определяемые особенностями элементов: элементы, подверженные воздействию электромагнитного поля (магнитные носители, микросхемы); программное обеспечение, подверженное программным конфликтам;

4) определяемые особенностями защищаемого объекта: местоположением объекта (отсутствие контролируемой зоны; реализация на нескольких удаленных друг от друга средствах вычислительной техники); организацией каналов обмена информацией (использование протоколов маршрутизации, использование глобальных инфокоммуникационных сетей, арендуемых каналов);

б) субъективные:

1) ошибки: при подготовке и использовании программного обеспечения (инсталляция и загрузка программного обеспечения, эксплуатация программного обеспечения, ввод данных); при управлении сложными системами (организация управления потоками обмена информации); при установке или эксплуатации технических средств и программного обеспечения;

2) нарушения: режима охраны и защиты (доступ к техническим средствам); режима эксплуатации технических средств (энергообеспечение, жизнеобеспечение); режима использования информации (обработка и обмен информацией, хранение и уничтожение информации); режима конфиденциальности;

в) случайные:

1) сбои и отказы: отказы и неисправности технических средств (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа); старение и размагничивание носителей информации (дискет и съемных носителей, жестких дисков, микросхем); сбои программного обеспечения; сбои электроснабжения;

2) повреждения: жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации; кондиционирования и вентиляции).

4.10.3.2.3 Источники дестабилизирующих воздействий

Источники, обусловленные действиями субъекта:

а) внешние источники:

1) случайные (непреднамеренные): персонал поставщиков услуг различного рода, персонал надзорных организаций и аварийных служб и др.;

2) преднамеренные: потенциальные преступники (террористы) и хакеры; недобросовестные партнеры; представители силовых структур (в чрезвычайных ситуациях);

б) внутренние источники: основной персонал; представители служб безопасности; обслуживающий персонал; технический персонал.

Источники, обусловленные действиями объекта:

а) внешние источники: технические и программные средства обработки информации при использовании глобальных инфокоммуникационных сетей;

б) внутренние источники: технические средства обработки информации; программные средства обработки информации; средства охраны.

Физические явления: пожары, землетрясения, ураганы, наводнения.

4.10.3.2.4 На уровне приложений, услуг и управления возможна реализация любых угроз согласно ГОСТ Р 52448. Возможными последствиями реализации угроз может быть нарушение любого из критериев безопасности сети электросвязи (конфиденциальность, целостность, доступность, подотчетность).

4.10.3.2.5 Возникновение уязвимостей на уровне инфраструктуры и линий железнодорожной электросвязи возможно на всех стадиях их жизненного цикла.

4.10.3.2.6 Реализация угроз, обусловленная действиями субъекта, характеристиками материальных объектов, физическими явлениями, возможна на стадии планирования, проектирования, строительства, эксплуатации, а также вывода из эксплуатации.

4.10.3.3 Критерии оценки безопасности уровня приложений, услуг и управления железнодорожной электросвязью:

- на стадии планирования: соответствие требованиям безопасности, предъявляемым стратегическими целями железнодорожной электросвязи;
- на стадии проектирования: соответствие характеристик проектируемых средств, систем, сетей и ресурсов железнодорожной электросвязи на уровне приложений, услуг и управления требованиям безопасности, предъявляемым на стадии планирования;
- на стадии эксплуатации и внедрения: соответствие заявленным поставщиком характеристикам;
- на стадии вывода из эксплуатации: соответствие требованиям безопасности по удалению и выводу из эксплуатации.

4.11 Обеспечение безопасности железнодорожной электросвязи в плоскостях управления

4.11.1 Меры обеспечения безопасности включают в себя:

- организационные (административные, экономические, юридические);
- технические (установка охранно-пожарной сигнализации, использование систем контроля и управления доступом, применение технических средств защиты информации, внедрение интегрированных систем безопасности);
- физические (работа сторожей и контролеров);
- оперативные (использование оперативных методов работы, оперативно-технических средств, например «полиграфа» для входного контроля и периодической проверки лояльности персонала).

4.11.2 Требования безопасности в плоскости административного управления определены [2] — [5].

5 Требования по обеспечению безопасности средств, систем и сетей железнодорожной электросвязи

5.1 Требования по обеспечению безопасности на уровне инфраструктуры железнодорожной электросвязи

5.1.1 Организационные требования безопасности

5.1.1.1 Необходимо наличие технической, нормативной и эксплуатационной документации на объектах инфраструктуры железнодорожной электросвязи.

5.1.1.2 На стадии эксплуатации должна проводиться регистрация в документах (журналах, актах, электронных базах данных) соответствующей информации о выполненных работах, состоянии объектов.

5.1.1.3 На стадии эксплуатации необходимо ограничение доступа к объектам инфраструктуры железнодорожной электросвязи.

5.1.1.4 На стадии эксплуатации необходимо вести учет лиц, получивших и использующих доступ к объектам инфраструктуры железнодорожной электросвязи.

5.1.2 Технические требования безопасности

5.1.2.1 Требования к элементам конструкции (к электрической прочности изоляции, устойчивость к воздействиям механических нагрузок и климатических факторов) должны выполняться согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7).

5.1.2.2 Требования к монтажу, эксплуатации и ремонту (крепление линий к сооружениям, строительство и прокладка) должны осуществляться в соответствии с утвержденным проектом; организация технического контроля в период строительства должна быть выполнена согласно [6] и ГОСТ Р ИСО/МЭК 17799 (раздел 7).

5.1.2.3 Требования к средствам защиты, сигнализации и контроля должны быть выполнены согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7).

5.1.2.4 Требования по обеспечению безопасности линий связи и направляющих систем должны соответствовать требованиям физической защиты и защиты от воздействия окружающей среды согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7).

5.1.3 Функциональные требования безопасности

Должны быть обеспечены защита от несанкционированного проникновения и доступность в обслуживании.

5.2 Требования по обеспечению безопасности на транспортном и функциональном уровнях железнодорожной электросвязи

5.2.1 Организационные требования безопасности

5.2.1.1 Необходимо наличие технической, нормативной и эксплуатационной документации на объекты транспортного уровня железнодорожной электросвязи.

5.2.1.2 На стадии эксплуатации необходима регистрация в документах (журналах, актах) соответствующей информации о выполненных работах, состоянии объектов.

5.2.1.3 На стадии эксплуатации необходимо ограничение доступа к объектам транспортного уровня железнодорожной электросвязи.

5.2.1.4 На стадии эксплуатации необходимо вести учет лиц, получивших и использующих доступ к объектам транспортного уровня железнодорожной электросвязи.

5.2.2 Технические требования безопасности

5.2.2.1 Требования к элементам конструкции (габариты, устойчивость к воздействиям механических нагрузок и климатических факторов) должны выполняться согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7).

5.2.2.2 Требования к монтажу, эксплуатации и ремонту (размещение в стойках, коробах; использование лицензионного программного обеспечения) должны выполняться согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7).

5.2.2.3 Требования к средствам защиты, сигнализации и контроля. Средства, системы, сети железнодорожной электросвязи транспортного уровня должны быть обеспечены средствами защиты, сигнализации и контроля в соответствии с требованиями политики безопасности, согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7). Оборудование железнодорожной электросвязи транспортного уровня должны иметь звуковую и световую сигнализацию, а также должно быть оснащено средствами контроля функционирования.

5.2.2.4 Не допускаются межсетевые незащищенные соединения и интерфейсы в первичных и вторичных сетях железнодорожной электросвязи, между элементами сети передачи данных и сетей оперативно-технологического и общетехнологического назначения.

5.2.3 Функциональные требования безопасности должны быть установлены согласно ГОСТ Р ИСО/МЭК 15408-2 (разделы 8, 10, 17).

5.3 Требования по обеспечению безопасности на уровне приложений, услуг и управления

5.3.1 Организационные требования безопасности

5.3.1.1 Необходимо наличие технической, нормативной, эксплуатационной и другой документации на средства, системы, сети и ресурсы железнодорожной электросвязи.

5.3.1.2 На стадии эксплуатации необходима фиксация в документах (журналах, актах, электронных базах данных) соответствующей информации о выполненных работах, состоянии эксплуатируемых объектов.

5.3.1.3 На стадии эксплуатации необходимо ограничение доступа к средствам, системам, сетям и ресурсам железнодорожной электросвязи.

5.3.1.4 На стадии эксплуатации необходимо вести учет лиц, получивших и использующих доступ к средствам, системам и сетям железнодорожной электросвязи.

5.3.2 Технические требования безопасности

5.3.2.1 Требования к эксплуатации (использование лицензионного программного обеспечения) должны быть выполнены согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7).

5.3.2.2 Требования к средствам защиты, сигнализации и контроля (обеспечение предупреждения о возникающих и реализованных угрозах, охват всех критичных систем) должны быть выполнены согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7).

5.3.3 Функциональные требования безопасности должны быть установлены согласно ГОСТ Р ИСО/МЭК 15408-2 (разделы 10, 14).

5.4 Требования и меры по обеспечению безопасности в плоскостях управления

5.4.1 Организационные требования и меры по обеспечению безопасности

5.4.1.1 Планирование безопасности

Безопасность должна соответствовать требованиям ГОСТ Р ИСО/МЭК 15408-2 (разделы 10, 12):

а) для каждого вида сетей и систем железнодорожной электросвязи должна быть разработана, утверждена, издана и доведена до сведения всех сотрудников организации, эксплуатирующей сеть или систему электросвязи, политика безопасности, которая должна определять:

1) ответственность руководства за обеспечение безопасности сетей и систем железнодорожной электросвязи;

2) общие и конкретные обязанности сотрудников по безопасности;

3) подход организации к управлению безопасностью;

4) систему обеспечения безопасности и функциональность службы безопасности;

б) по мере изменения направлений деятельности и бизнес-целей организации политика безопасности должна корректироваться.

План безопасности должен ежегодно разрабатываться, утверждаться руководством организации, эксплуатирующей сеть или систему железнодорожной электросвязи.

5.4.1.2 Требования по безопасности персонала должны выполняться согласно ГОСТ Р ИСО/МЭК 17799 (раздел 6):

а) должны быть определены категории персонала, связанного с обработкой, хранением и передачей информации и установлены критерии отбора для лиц, претендующих на эти должности;

б) должны быть установлены правила поведения персонала, эксплуатирующего средства информационных технологий, в отношении обеспечения безопасности, описывающие обязанности персонала и ожидаемые от него действия по обеспечению безопасности;

в) до сведения персонала, подвергаемого отбору до его допуска к работе, должны быть доведены (под роспись) правила поведения и ответственность за нарушение режима безопасности, а после завершения контракта — ответственность за сохранность полученных в ходе работы сведений;

г) персонал должен быть обучен требованиям безопасности, в том числе и защите от несанкционированного доступа до разрешения доступа персонала к работе;

д) необходимо периодически осуществлять переподготовку персонала и регулярно проводить мероприятия по его информированию о необходимости соблюдения установленных требований безопасности.

5.4.1.3 Физическая безопасность

Должен быть определен порядок контроля всех физических точек доступа на объекты инфраструктуры железнодорожной электросвязи (включая двери, окна, места ввода в сооружения связи элементов систем вентиляции, канализации, водоснабжения, газоснабжения, электроснабжения и телекоммуникаций) согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7).

Должен осуществляться мониторинг физического доступа в помещения, в которых размещаются технические средства, согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7).

Должна осуществляться регистрация действий персонала по обслуживанию технических средств согласно ГОСТ Р ИСО/МЭК 17799 (раздел 6).

Порядок передачи оборудования другим организациям и его утилизации должен быть определен в отдельной инструкции, устанавливающей действия по недопущению наличия в устройствах хранения

информации, передаваемых или подлежащих утилизации программно-аппаратных средств, остаточной информации согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7) и [7].

В процессе мониторинга физического доступа в помещения, в которых размещаются технические средства, должны использоваться устройства видеонаблюдения и сигнализации реального времени. Должны использоваться автоматизированные средства регистрации действий персонала по обслуживанию технических средств [7, 8].

5.4.1.4 Планирование действий при чрезвычайных ситуациях должно выполняться согласно ГОСТ Р ИСО/МЭК 17799 (разделы 6, 7) и [7].

В организации, эксплуатирующей средства, системы, сети железнодорожной электросвязи, должен разрабатываться и осуществляться план мероприятий в чрезвычайных ситуациях, в том числе и при террористических актах, учитывая функции и обязанности персонала и действия, связанные с восстановлением систем после выхода из строя их элементов.

Персонал должен быть обучен действиям в чрезвычайных ситуациях, и должна осуществляться его переподготовка.

Проверка плана действий в чрезвычайных ситуациях и его корректировка должны проводиться не реже одного раза в год с целью определения эффективности и готовности организации к выполнению данного плана.

Должно проводиться резервное копирование и хранение в защищенном виде критической информации пользователей и системы управления.

5.4.1.5 Реагирование на инциденты безопасности должно выполняться согласно ГОСТ Р ИСО/МЭК 17799 (раздел 6) и [7].

В организации, эксплуатирующей средства, системы, сети железнодорожной электросвязи, должен разрабатываться и осуществляться план мероприятий по обработке инцидентов безопасности и проводиться его корректировка не реже одного раза в год с целью определения эффективности и готовности организации к выполнению данного плана.

Должна осуществляться подготовка к возможному проявлению инцидента, его предупреждению, обнаружению, реагированию, сдерживанию, устранению и восстановлению исходного состояния.

Должна быть определена группа специалистов служб безопасности и информационных технологий, способных реагировать на инциденты в области информационной безопасности, которые должны иметь возможность устного (по телефону) или письменного (по электронной почте) обмена информацией с пользователями услугами связи, взаимодействующими операторами связи и органами безопасности государства и обеспечения правопорядка о нарушениях безопасности, которые могут перерасти в инцидент безопасности.

Должно быть предусмотрено привлечение внешних служб реагирования на инциденты.

5.4.2 Функциональные требования и меры по обеспечению безопасности

5.4.2.1 Идентификация и аутентификация

Для персонала, осуществляющего управление, настройку и конфигурирование аппаратных средств информационных и телекоммуникационных технологий, должны обеспечиваться идентификация и аутентификация при их доступе к данным средствам согласно ГОСТ Р ИСО/МЭК 15408-2 (раздел 11).

При удаленном доступе к аппаратным средствам взаимодействующих систем и сетей со стороны обслуживающего персонала должна обеспечиваться идентификация оконечного оборудования.

Для каждого сеанса удаленного доступа должно обеспечиваться установление уникальных параметров аутентификации.

Защита от несанкционированного доступа к программно-аппаратным средствам, с помощью которых предоставляются услуги сети передачи данных, оказываемых пользователям сетей передачи данных, должна включать процедуру аутентификации пользователей согласно ГОСТ Р ИСО/МЭК 17799 (раздел 9).

5.4.2.2 Контроль доступа

При управлении, настройке, конфигурировании программно-аппаратных средств (включая доступ к оконечному кабельному и распределительному оборудованию) и обслуживании абонентских линий, для персонала, эксплуатирующего указанные средства, должны быть установлены контроль, регистрация и ограничение его действий в соответствии с установленными полномочиями на доступ к средствам, их программному обеспечению, приложениям и данным. Должен быть осуществлен запрет подобных действий для посторонних лиц или доступ с паролем по умолчанию (введенным производителем оборудования или программного обеспечения).

Ограничение доступа должно осуществляться мерами контроля доступа, определяющими:

- объекты, санкционированные к получению доступа, и средства, к которым данные объекты уполномочены иметь доступ;

- разрешения по типу доступа (чтение, запись, изменение, создание, удаление).

Полномочия (права) доступа персоналу, сменившему рабочие места или покинувшему организацию, должны своевременно удаляться.

Полномочия (права) доступа должны назначаться персоналу в минимально необходимом объеме в соответствии с их приоритетами, функциями и обязанностями и не реже одного раза в шесть месяцев пересматриваться. При этом рекомендуется использовать только персональные учетные записи.

5.4.2.3 Обеспечение конфиденциальности

Для управляющей информации данными конфигурирования программно-аппаратных средств информационных и телекоммуникационных технологий при ее передаче по каналам связи и хранении должен быть определен порядок обеспечения ее сохранности от доступа к ней несанкционированных лиц согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7) и [7, 9].

5.4.2.4 Аудит событий безопасности — согласно ГОСТ Р ИСО/МЭК 15408-2 (раздел 7), ГОСТ Р ИСО/МЭК 17799 (раздел 12) и [7].

В целях проверки зарегистрированных данных, касающихся событий несанкционированного доступа и выявления причин и условий, способствующих нарушению целостности и устойчивости функционирования систем и сетей железнодорожной электросвязи, должна обеспечиваться возможность их анализа.

Журналы регистрации событий, имеющих отношение к безопасности систем и сетей железнодорожной электросвязи, должны храниться в течение достаточного срока для обеспечения расследований инцидентов. Срок хранения журналов регистрации событий должен определяться исходя из сроков исковой давности.

Для любого публично доступного сетевого ресурса в системах и сетях железнодорожной электросвязи должна быть представлена возможность получения информации о его владельце в объеме, разрешенном законодательством.

Для фильтрации потока первичных событий, регистрируемых в журналах, рекомендуется применять средства корреляции событий, оптимизирующие записи в журналах инцидентов по безопасности.

5.4.2.5 Подотчетность

Регистрация действий в сети участников сетевого взаимодействия должна обеспечивать возможность получения документального подтверждения этих действий согласно ГОСТ Р ИСО/МЭК 17799 (раздел 8) и [7].

5.4.2.6 Целостность данных и программных средств должна быть обеспечена согласно ГОСТ Р ИСО/МЭК 17799 (раздел 8), ГОСТ Р ИСО/МЭК 15408-2 (подраздел 10.11).

Для обеспечения целостности хранимых и передаваемых данных, защиты их от модификации, уничтожения, создания (вставки) и повторной передачи должна быть исключена возможность неконтролируемого доступа к ним со стороны обслуживающего персонала.

В системах и сетях железнодорожной электросвязи должна отсутствовать возможность удаленного воздействия на порты сетевого оборудования, связанные с его конфигурированием.

В системах и сетях железнодорожной электросвязи должна обеспечиваться целостность программного обеспечения средств связи, включающая использование лицензионной антивирусной защиты, с обеспечением возможности автоматических обновлений, для обнаружения и уничтожения злонамеренного кода (вирусов и др.).

Должно обеспечиваться централизованное управление механизмами антивирусной защиты.

5.4.2.7 Безопасность инфраструктуры должна быть обеспечена согласно ГОСТ Р ИСО/МЭК 17799 (раздел 7) и [7], [8], [9].

Технические средства, используемые для передачи, обработки и (или) хранения управляющей информации, должны быть физически изолированы от вспомогательных (обеспечивающих) технических средств.

Для любого аппаратного оборудования и (или) программного обеспечения должны приниматься меры по установке рекомендованных изготовителем обновлений и (или) в кратчайшие сроки должно осуществляться уведомление пользователей об обнаруженных уязвимостях используемого оборудования и (или) программного обеспечения, а также о нарушениях системы безопасности, которые могут иметь последствия для систем и сетей железнодорожной электросвязи.

Подключения сетей железнодорожной электросвязи к сетям, имеющим выход на сети общего пользования и сети передачи данных, должны осуществляться только через межсетевое экранирование и быть снабжены сертифицированными средствами обнаружения вторжения и антивирусной защиты.

В системах и сетях железнодорожной электросвязи должен быть определен перечень составных компонентов и элементов, требующих защиты.

Средства защиты информации, используемые в системах и сетях железнодорожной электросвязи, должны иметь действующие сертификаты (аттестаты) соответствия и проходить предусмотренные процедуры проверки.

В системах и сетях железнодорожной электросвязи не должны использоваться меры безопасности, которые наносят вред непричастным субъектам информационного обмена. Используемые программно-аппаратные средства защиты не должны ухудшать характеристики основных технических средств.

6 Требования к железнодорожной электросвязи, ее составным частям и элементам составных частей по обеспечению безопасности

6.1 Требования к железнодорожной электросвязи по обеспечению безопасного движения железнодорожного подвижного состава с установленной скоростью и минимальным интервалом следования

6.1.1 Требования функциональной безопасности и надежности

6.1.1.1 Должны быть обеспечены защита от несанкционированного проникновения и доступность в обслуживании согласно ГОСТ Р ИСО/МЭК 17799 (раздел 9).

6.1.1.2 Требования функциональной безопасности на функциональном и транспортном уровне железнодорожной электросвязи должны быть установлены согласно ГОСТ Р ИСО/МЭК 15408-2 (разделы 8, 10, 17).

6.1.1.3 Требования функциональной безопасности на уровне приложений, услуг и управления железнодорожной электросвязью должны быть установлены согласно ГОСТ Р ИСО/МЭК 15408-2 (разделы 10, 14) и ГОСТ Р 61508-2 (раздел 7).

6.1.2 Требования информационной безопасности должны выполняться, согласно 5.4 и соответствовать требованиям, установленным ГОСТ Р 52448 (раздел 6) и ГОСТ Р ИСО/МЭК 13335-1 (раздел 10).

6.1.3 Требования к организационной и физической безопасности

6.1.3.1 Организационные требования безопасности на уровне инфраструктуры железнодорожной электросвязи установлены в 5.1.1 и должны соответствовать требованиям согласно ГОСТ Р 27001 (раздел 4).

6.1.3.2 Организационные требования безопасности на функциональном и транспортном уровне железнодорожной электросвязи установлены в 5.2.1 и должны соответствовать требованиям согласно ГОСТ Р 27001 (раздел 4).

6.1.3.3 Организационные требования безопасности на уровне приложений, услуг и управления железнодорожной электросвязью установлены в 5.3.1 и должны соответствовать требованиям согласно ГОСТ Р 27001 (раздел 4).

6.1.3.4 Организационные требования и меры безопасности в плоскостях управления железнодорожной электросвязью установлены в 5.4.1 и должны соответствовать требованиям согласно ГОСТ Р 27001 (раздел 4).

6.2 Требования к железнодорожной электросвязи по обеспечению мониторинга параметров функционирования и интегрированного управления технологической сетью связи и частотно-временной синхронизации

6.2.1 Требования по обеспечению безопасности на уровне инфраструктуры железнодорожной электросвязи согласно 5.1.1—5.1.3.

6.2.2 Требования по обеспечению безопасности на уровне транспорта/передачи и функциональном уровне (маршрутизация, коммутация, доступ) железнодорожной электросвязи согласно 5.2.1—5.2.3.

6.2.3 Требования по обеспечению безопасности средств, систем, сетей и видов железнодорожной электросвязи на уровне приложений, услуг и управления согласно 5.3.1—5.3.3.

6.2.4 Требования к сети частотно-временной синхронизации, согласно [10].

6.2.5 Средства и системы железнодорожной электросвязи уровня приложений, услуг и управления должны иметь в своем составе защищенные системы мониторинга и администрирования согласно 4.10.3.1.

6.3 Требования совместимости подсистемы железнодорожной электросвязи с другими подсистемами инфраструктуры железнодорожного транспорта и железнодорожным подвижным составом

Системы и средства железнодорожной электросвязи должны соответствовать требованиям помехоустойчивости, установленным применительно к различным портам аппаратуры железнодорожной электросвязи, при воздействии:

- электростатических разрядов — в соответствии с ГОСТ Р 51317.4.2 (разделы 4 и 5);
- наносекундных импульсных помех — в соответствии с ГОСТ Р 51317.4.4 (разделы 4—7);
- микросекундных импульсных помех большой энергии — в соответствии с ГОСТ Р 51317.4.5 (разделы 3—5);
- динамических изменений напряжения электропитания — в соответствии с ГОСТ Р 51317.4.11 (раздел 6 и приложение Б);
- радиочастотного электромагнитного поля — в соответствии с ГОСТ Р 51317.4.3 (раздел 5 и приложение А);
- магнитного поля промышленной частоты — в соответствии с ГОСТ Р 50648 (раздел 5);
- кондуктивных помех в полосе частот от 0,15 до 80 МГц, наведенных радиочастотными электромагнитными полями, — в соответствии с ГОСТ Р 51317.4.6 (раздел 5);
- кондуктивных помех в полосе частот от 0 до 150 кГц — в соответствии с ГОСТ Р 51317.4.16 (раздел 5 и приложение А).

6.4 Требования по сохранению работоспособного состояния железнодорожной электросвязи во всех предусмотренных при проектировании условиях и режимах в течение установленных сроков службы

6.4.1 Требования по обеспечению безопасности на уровне инфраструктуры железнодорожной электросвязи — согласно 5.1.2.

6.4.2 Требования по обеспечению безопасности на уровне транспорта/передачи и функциональном уровне (маршрутизация, коммутация, доступ) железнодорожной электросвязи — согласно 5.2.2.

6.4.3 Требования по обеспечению безопасности средств, систем, сетей и видов железнодорожной электросвязи на уровне приложений, услуг и управления — согласно 5.3.2.

Приложение А
(рекомендуемое)

Перечень основных угроз

Таблица А.1

Наименование	Источник угрозы/категория нарушителя	Используемые уязвимости (пример)
Сбои и ошибки в работе программного обеспечения и телекоммуникационного оборудования	Форс-мажорные обстоятельства	Несвоевременная установка обновлений программного обеспечения. Недостаточная координация действий подразделений эксплуатации и технической поддержки
Техногенные явления (пожар, наводнение)	Форс-мажорные обстоятельства	Особенности расположения. Несоблюдение мер противопожарной безопасности. Отсутствие плана действий в чрезвычайных ситуациях
Кража/вандализм	Внешние/внутренние злоумышленники	Отсутствует система физической безопасности
Сбои и ошибки в работе программного обеспечения	Форс-мажорные обстоятельства	Недостаточная координация действий подразделений эксплуатации и подразделений технической поддержки
Разрушение канала связи	Форс-мажорные обстоятельства	Размещение кабеля на неконтролируемой территории
Сбой в сети электропитания	Форс-мажорные обстоятельства.	Отсутствие резервного питания
Сбой в работе системы вентиляции и кондиционирования	Форс-мажорные обстоятельства. Внешние/внутренние злоумышленники	Отсутствие стандартов на размещение оборудования на территории организации. Отсутствие обслуживания оборудования, осуществляющего кондиционирование воздуха
Ошибки персонала	Сотрудники организации	Недостаточная компетенция пользователей. Недостаточно ответственный подход к работе. Отсутствие поддержки пользователей
Нехватка персонала	Сотрудники организации	Недостаточное финансирование. Неблагоприятные производственные отношения
Недостаточность функциональных характеристик	Производители оборудования и программного обеспечения	Отсутствие средств защиты системы от превышения ограничений по ресурсам (объем оперативной памяти, жестких дисков, пропускная способность и т. п.)
Фальсификация полномочий	Внешние/внутренние злоумышленники	Использование недостаточно сложных паролей
Злоупотребление полномочиями	Внешние/внутренние злоумышленники	Использование недостаточно сложных паролей. Возможность удаленного администрирования системы. Сложность и неудобство назначения прав
Применение вредоносного программного обеспечения	Внешние/внутренние злоумышленники	Наличие недекларированных возможностей, добавленных на этапах проектирования и разработки. Возможность модификации или повреждения программного обеспечения

Продолжение таблицы А.1

Наименование	Источник угрозы/категория нарушителя	Используемые уязвимости (пример)
Недопустимое использование оборудования	Внешние/внутренние злоумышленники	Неопределение ответственности за обеспечение безопасности информационной системы. Возможность установки вредоносного программного обеспечения на операционную систему
Отказ от действий	Внешние/внутренние злоумышленники	Отсутствие регистрации событий. Не использование системы ведения системных событий
Сбой в работе внешнего сервиса	Поставщики сервиса	Отсутствие в договорах положений, регулирующих максимально допустимое время простоя важных сервисов
Угрозы уровня сетевых интерфейсов	Форс-мажорные обстоятельства	Неконтролируемый физический доступ к среде передачи данных, позволяющий осуществить атаку типа «отказ в обслуживании» с нарушением целостности физической среды передачи данных
Угрозы уровня межсетевых взаимодействий	Внешние/внутренние злоумышленники	Не применяются средства криптографической защиты информации, что позволяет осуществить перехват и модификацию информации, передаваемой по каналам связи. Отсутствуют средства контроля целостности передаваемой информации, что позволяет осуществить перехват и модификацию информации, передаваемой по каналам связи
Угрозы уровня приложений	Внешние/внутренние злоумышленники	Использование уязвимых версий программного обеспечения на активном сетевом оборудовании, серверах и рабочих станциях, позволяющее получить несанкционированный доступ к активному сетевому оборудованию и сервисам. Отсутствие средства контроля доступа, позволяющее получить несанкционированный доступ к активному сетевому оборудованию и сервисам с использованием метода подбора пароля (в том числе в комбинации с атакой типа «отказ в обслуживании», направленной на серверы аутентификации)
Нарушение функционирования служб DNS, SMTP, SNMP	Внешние/внутренние злоумышленники	Некорректные настройки штатных механизмов защиты программного обеспечения. Отсутствие дополнительных мер и средств защиты. Несвоевременная установка обновлений программного обеспечения
Модификация файлов конфигурации телекоммуникационного оборудования	Внешний/внутренний нарушитель	Отсутствие разделения полномочий. Недостаточность регистрируемых системой аудита событий. Недостаточный контроль над действиями персонала подразделений эксплуатации. Отсутствие дополнительных мер и средств защиты
Ознакомление с проектной и нормативно-технической документацией на систему	Внешний нарушитель	Отсутствие разделения полномочий. Отсутствие регламента хранения и доступа к документации

Продолжение таблицы А.1

Наименование	Источник угрозы/категория нарушителя	Используемые уязвимости (пример)
Получение информации о состоянии телекоммуникационного оборудования	Внешний/внутренний нарушитель	Недостаточный контроль над действиями персонала подразделений эксплуатации. Отсутствие категорирования информации, контроля доступа и аудита
Разрушение канала связи	Внешний/внутренний нарушитель	Размещение кабеля на неконтролируемой территории
Нарушение штатного функционирования	Диверсия	Недостаточный контроль над действиями персонала подразделений эксплуатации
Нарушение условий соглашения о конфиденциальности и разглашение материалов проекта (документации)	Внешний/внутренний нарушитель	Предоставление разработчику избыточной информации. Отсутствие механизмов контроля соблюдения условий конфиденциальности
Некорректное обращение с каналом доступа	Разработчик	Недостаточность регистрируемых системой аудита событий. Отсутствие контроля и фиксации действий персонала технической поддержки. Отсутствие дополнительных мер и средств защиты
Модификация файлов конфигурации телекоммуникационного оборудования	Внешний сотрудник технической поддержки	Отсутствие разделения полномочий. Недостаточность регистрируемых системой аудита событий. Отсутствие контроля и фиксации действий персонала технической поддержки. Отсутствие дополнительных мер и средств защиты
Модификация файлов конфигурации системного программного обеспечения	Внешний сотрудник технической поддержки	Отсутствие разделения полномочий. Недостаточность регистрируемых системой аудита событий. Отсутствие дополнительных мер и средств защиты
Модификация файлов конфигурации телекоммуникационного оборудования	Внутренний сотрудник технической поддержки (администратор)	Отсутствие разделения полномочий. Недостаточность регистрируемых системой аудита событий. Отсутствие контроля и фиксации действий персонала технической поддержки. Отсутствие дополнительных мер и средств защиты
Нарушение функционирования сервисов системы управления	Внутренний сотрудник технической поддержки (администратор)	Отсутствие разделения полномочий. Недостаточный контроль над действиями персонала подразделений эксплуатации центрального офиса. Отсутствие дополнительных мер и средств защиты
Модификация журналов аудита	Внутренний сотрудник технической поддержки (администратор сети)	Отсутствие разделения полномочий. Отсутствие дополнительных мер и средств защиты
Модификация файлов конфигурации телекоммуникационного оборудования	Администратор	Отсутствие разделения полномочий. Недостаточность регистрируемых системой аудита событий. Отсутствие контроля и фиксации действий персонала технической поддержки
Модификация журналов аудита	Администратор	Отсутствие разделения полномочий. Отсутствие резервного копирования журналов аудита и их защиты

Окончание таблицы А.1

Наименование	Источник угрозы/категория нарушителя	Используемые уязвимости (пример)
Модификация файлов конфигурации системного программного обеспечения	Администратор дежурной смены	Отсутствие разделения полномочий. Недостаточность регистрируемых системой аудита событий. Отсутствие дополнительных мер и средств защиты
Модификация файлов конфигурации телекоммуникационного оборудования	Администратор дежурной смены	Отсутствие разделения полномочий. Недостаточность регистрируемых системой аудита событий. Отсутствие дополнительных мер и средств защиты
Утрата дистрибутивов программного обеспечения системы управления	Администратор дежурной смены	Отсутствие разделения полномочий. Отсутствие регламента доступа к дистрибутивам программного обеспечения
Нарушение функционирования сервисов системы управления	Внутренний сотрудник технической поддержки (администратор сети)	Отсутствие разделения полномочий. Недостаточный контроль над действиями персонала подразделений эксплуатации. Отсутствие дополнительных мер и средств защиты
Нарушение функционирования сервиса точного времени	Администратор дежурной смены	Отсутствие разделения полномочий. Недостаточный контроль над действиями персонала подразделений эксплуатации. Отсутствие дополнительных мер и средств защиты
Нарушение функционирования: VLAN системы удаленного управления, сервисов межсетевого экранирования трафика VLAN мониторинга сетевых элементов сети	Администратор дежурной смены	Отсутствие разделения полномочий. Недостаточность регистрируемых системой аудита событий. Отсутствие дополнительных мер и средств защиты
Несанкционированное подключение к телекоммуникационному оборудованию	Администратор дежурной смены	Отсутствие разделения полномочий. Недостаточный контроль за действиями персонала подразделений эксплуатации. Отсутствие дополнительных мер и средств защиты

Библиография

[1] Рекомендация МСЭ-Т X.805 — Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами

[2] Рекомендация МСЭ-Т M.3016.1:2005 — Безопасность для плоскости административного управления: Требования безопасности

[3] Рекомендация МСЭ-Т M.3016.2 — Безопасность для плоскости административного управления: Услуги по обеспечению безопасности

[4] Рекомендация МСЭ-Т M.3016.3 — Безопасность для плоскости административного управления: Механизм безопасности

[5] Рекомендация МСЭ-Т M.3016.4 — Безопасность для плоскости административного управления: Проформа структуры

[6] Правила подвески и монтажа самонесущего волоконно-оптического кабеля на опорах контактной сети и высоковольтных линий автоблокировки (утверждены МПС РФ 16.08.1999 г., № ЦЭ/ЦИС-677)

[7] Указ Президента Российской Федерации № 351 от 17 марта 2008 г. «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

[8] Перечень критически важных объектов Российской Федерации (утвержден распоряжением Правительства Российской Федерации от 23 марта 2006 г. № 411-рс)

[9] Федеральный закон Российской Федерации от 7 июля 2003 г. № 126-ФЗ «О связи»

[10] Правила построения оборудования тактовой сетевой синхронизации (утверждены Минсвязи России 07.12.2006 г., № 161)

УДК 621.39:006.354 ОКС 45.020 ОКП 31 8560

Ключевые слова: безопасность, требования безопасности, железнодорожная электросвязь

Редактор *Е.С. Котлярова*
Технический редактор *Н.С. Гришанова*
Корректор *Ю.М. Прокофьева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 19.12.2012. Подписано в печать 17.01.2013. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 3,15. Тираж 83 экз. Зак. 39.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.