ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53109— 2008

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Паспорт организации связи по информационной безопасности

Издание официальное

БЗ 12—2008/541

Москва
Стандартинформ
2009

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 Федеральным государственным унитарным предприятием «Центральный научно-исследовательский институт связи» (ФГУП «ЦНИИС»), Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»)

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 527-ст

4 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

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Паспорт организации связи по информационной безопасности

Information security of the public communications network providing system. Passport of the organization communications of information security

Дата введения — 2009—10—01

1 Область применения

Настоящий стандарт устанавливает требования к форме и содержанию паспорта организации связи по информационной безопасности относительно сети (сетей) электросвязи.

Паспортизации по требованиям к информационной безопасности подлежат все организации связи, независимо от организационной правовой формы собственности, являющиеся частью производственной инфраструктуры связи Российской Федерации и функционирующие на ее территории как взаимоувязанный производственно-хозяйственный комплекс, предназначенный для оказания услуг связи, предоставляемых с использованием сети связи общего пользования, гражданам, органам государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

Паспорт организации связи по информационной безопасности представляет собой документированное подтверждение реализации общеобязательных правовых норм по информационной безопасности, осуществляемых в соответствии с положениями:

- законов Российской Федерации;
- указов и распоряжений Президента Российской Федерации;
- постановлений и распоряжений Правительства Российской Федерации;
- нормативных правовых актов (приказов, распоряжений) ФОИВ, уполномоченных в областях связи, обеспечения безопасности и технической защиты информации;
- национальных стандартов, стандартов организаций, сводов правил, систем добровольной сертификации в области информационной безопасности сетей электросвязи.

Проведение паспортизации организаций связи на основе определения, обобщения и представления в документированном виде всех данных, определяющих состояние информационной безопасности инфокоммуникационной структуры сети (сетей) электросвязи, должно существенно повысить эффективность системы обеспечения информационной безопасности, чтобы гарантировать пользователям доступность услуг связи с заданным уровнем качества.

Паспорт организации связи по информационной безопасности должен являться подтверждением способности оператора связи:

- соблюдать права пользователей услугами связи на доступ к информации при обеспечении конституционных прав и свобод человека и гражданина на персональную тайну, тайну связи (тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений);
- противостоять угрозам безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

Издание официальное

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

ГОСТ Р 53110—2008 Система обеспечения информационной безопасности сети связи общего пользования. Общие положения

ГОСТ Р 53111—2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки

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 следующие термины с соответствующими определениями:

3.1

оператор связи: Юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии.

[Закон РФ «О связи», статья 2, пункт 12]

3.2

организация связи: Юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность в области связи в качестве основного вида деятельности.

[Закон РФ «О связи», статья 2, пункт 14]

3.3 **политика информационной безопасности оператора связи:** Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области обеспечения информационной безопасности, которыми должен руководствоваться оператор связи.

3.4

сеть связи: Технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи.

[Закон РФ «О связи», статья 2, пункт 24]

3.5

система обеспечения информационной безопасности сети (сетей) электросвязи: Совокупность организационно-технической структуры и(или) исполнителей, задействованных в обеспечении информационной безопасности сети (сетей) электросвязи и используемых ими механизмов обеспечения безопасности (средств защиты), взаимодействующая с органами управления сетью (сетями) связи, функционирование которой осуществляется по нормам, правилам и обязательным требованиям, установленным федеральными органами исполнительной власти, уполномоченными в областях связи, обеспечения безопасности и технической защиты информации.

[ГОСТ Р 53110, пункт 3.6]

3.6

служба информационной безопасности организации связи: Организационно-техническая структура организации связи, реализующая политику информационной безопасности организации связи и осуществляющая функционирование системы обеспечения информационной безопасности сети (сетей) электросвязи.

[ГОСТ Р 53110, пункт 3.7]

3.7

системный проект сети связи: Схема построения сети электросвязи с соответствующими такой схеме расчетными значениями (с учетом предъявляемых к сети электросвязи обязательных требований и планируемого объема оказываемых услуг связи) величин, определяющих технические возможности входящих в состав сети электросвязи средств связи, линий передачи и физических цепей, и монтированной емкости.

[Закон РФ «О связи», статья 2, пункт 26]

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ВН — воздействие нарушителя;
ГИИ — глобальная информационная инфраструктура;
ИБ — информационная безопасность;
ИТ — информационная технология;
НСД — несанкционированный доступ;
ПДК по ИБ — постоянно действующая комиссия по ИБ;
ПО — программное обеспечение;
СМИБ — система менеджмента информационной безопасности;
СОИБ — система обеспечения информационной безопасности;
ФОИВ — федеральный орган исполнительной власти;
ЭМ ВОС — эталонная модель взаимосвязи открытых систем.

5 Форма паспорта организации связи по информационной безопасности

5.1 Паспорт организации связи по ИБ разрабатывается в соответствии с ГОСТ Р 52448 и его форма и содержание в организациях связи в зависимости от специфики их функционирования могут быть различными. Сведения, включенные в паспорт, должны периодически уточняться и обновляться.

5.2 Основой разработки формы и содержания паспорта являются результаты проведенного анализа состояния защищенности инфокоммуникационной структуры сети (сетей) электросвязи организации связи, определения наиболее критичных к ВН объектов ИБ, уязвимостей структурных компонентов сети (сетей), возможных угроз и реализации требований ИБ.

5.3 Пример формы паспорта организации связи по ИБ приведен в приложении А.

6 Формирование исходных данных

6.1 Составление паспорта

Составление паспорта осуществляется комиссией[1)] в составе пяти — семи квалифицированных специалистов связи, ИТ структур и службы ИБ, назначаемой приказом руководителя организации связи. Председателем комиссии назначают заместителя руководителя организации связи (начальника службы ИБ).

Комиссия, используя системный проект сети связи [1], осуществляет обследование инфокоммуникационной структуры сети (сетей) электросвязи организации связи, которое предполагает проведение мероприятий и действий, перечисленных в 6.1.1 — 6.1.8.

6.1.1 Категорирование сети (сетей) электросвязи

Сети электросвязи для предъявления к ним требований ИБ подразделяют на следующие категории:

- высшая;
- средняя;
- низшая.

В качестве примера в приложении Б приведены категории сетей электросвязи по защите от НСД [2] в зависимости от типов категорий узлов связи.

[1)] Роль комиссии по составлению паспорта может выполнять ПДК по ИБ организации связи.

Категорию сети электросвязи по требованиям ИБ (защите от НСД) устанавливают актом о категорировании сети электросвязи (см. приложение В). Комиссия составляет пояснительную записку к акту, содержащую сведения о мерах обеспечения безопасности, которые реализуют требования ИБ (защиты от НСД), соответствующие установленной категории сети электросвязи.

6.1.2 Проведение анализа условий функционирования организации связи

Анализ условий функционирования организации связи отображают в разделе А.2 паспорта (см. приложения А) «Ситуационный план организации связи».

Ситуационный план организации связи может быть сформирован на основе генерального плана организации и представлен отдельным приложением к паспорту с пояснительной запиской. Примерный состав пояснительной записки к ситуационному плану представлен в 6.2.

6.1.3 Проведение инвентаризации информационных ресурсов

Инвентаризация предполагает описание информационных ресурсов в соответствии с перечнем, приведенным в пункте А.3.1 паспорта (см. приложение А) «Информационные ресурсы, требующие защиты».

6.1.4 Исследование инфраструктуры сети (сетей) электросвязи

В пункте А.3.2.1 паспорта «Структура сети (сетей) электросвязи» (см. приложение А) необходимо указать тип сети (сетей): транзитная(ые), международная(ые), междугородная(ые), зоновая(ые), местная(ые), локальная(ые), выделенная(ые), технологическая(ие), сеть (сети) радиосвязи, специальные и др., а также привести структурную схему сети (сетей) электросвязи с указанием узлов сопряжения с ГИИ, в том числе с сетью Интернет. Необходимо также в паспорте указать защищенные системы и линии связи, в том числе по радиорелейным и спутниковым каналам связи. Сетевая структура организации связи отражается также в «карте сети», порядок составления которой приведен в приложении Г.

6.1.5 Составление перечня средств связи

В перечень включают средства связи, влияющие на обеспечение ИБ, с определением мест их установки (населенный пункт, комната, этаж, здание) и условий обеспечения (электропитание, заземление, открытые и защищенные коммуникации, в том числе имеющие выход за пределы контролируемой зоны), при этом:

- определяют технические средства и системы, применение которых не обосновано служебной или производственной необходимостью и которые подлежат демонтажу, а также технические средства, не влияющие на уровень обеспечения ИБ;

- определяют технические средства, требующие переоборудования и дополнительной защиты;

- составляют перечень основных средств связи, участвующих в процессе обработки, хранения и передачи информации/данных. Пункт А.3.2.2 паспорта (см. приложение А) должен содержать описательную часть, таблица А.1 паспорта (см. приложение А) — перечень рассматриваемых основных средств связи. Перечень должен соответствовать номенклатуре средств связи, подлежащих сертификации (подтверждению соответствия). В перечне основных средств связи должно быть выделено оборудование, предназначенное для обработки, хранения и передачи информации управления и персональных данных пользователей услугами связи;

- составляют перечень вспомогательных средств связи в соответствии с таблицей А.2 паспорта (см. приложение А), к которым должны относиться средства связи, непосредственно не участвующие в процессе обработки, хранении и передачи информации, но размещенные совместно с основными средствами и системами, участвующими в этом процессе.

Примечание — В таблицах А.1 и А.2 паспорта (см. приложение А) в графе «примечание» должны быть указаны сведения (при наличии) о сертификации, специсследованиях и спецпроверках технических средств.

6.1.6 Уточнение сведений об используемом программном обеспечении

В таблице А.3 паспорта (см. приложение А) приводится перечень используемого ПО (операционные системы, сетевое и прикладное ПО, базы данных и т.д.)

6.1.7 Уточнение сведений об используемых протоколах информационного обмена

В пункте А.3.2.5 паспорта (см. приложение А) должны быть перечислены используемые в сети (сетях) электросвязи протоколы информационного обмена. Протоколы должны быть разграничены по уровням ЭМ ВОС, также необходимо выделить используемые защищенные криптографические протоколы.

6.1.8 Уточнение схем размещения основных средств связи

В пункте А.3.2.6 паспорта (см. приложение А) должны быть приведены схемы размещения основных средств связи на объектах организации связи с привязкой к границам контролируемых зон.

6.2 Пояснительная записка к ситуационному плану организации связи

Пояснительная записка к Ситуационному плану организации связи составляется службой ИБ организации связи и должна содержать развернутое описание представленных в 6.2.1 — 6.2.4 структурных компонентов.

6.2.1 Перечень объектов ИБ инфокоммуникационной структуры сети (сетей) электросвязи

При составлении перечня объектов ИБ инфокоммуникационной структуры сети (сетей) электросвязи необходимо учитывать, что для сетей электросвязи объекты ИБ представляют собой аппаратные и программные средства, входящие в состав сетей, а также информационные ресурсы, ВН на которые может привести к последствиям, связанным с нарушением основных критериев ИБ — конфиденциальности, целостности, доступности и подотчетности.

К основным объектам ИБ сети (сетей) электросвязи могут быть отнесены:

- информационные ресурсы;
- узлы абонентского доступа;
- технические средства обработки, хранения и передачи информации;
- линии электросвязи, ПО;
- базы данных, системы управления базами данных;
- серверы, рабочие станции;
- системы управления сетями электросвязи, системы сигнализации;
- протоколы информационного обмена;
- механизмы обеспечения безопасности (средства защиты).

6.2.2 Перечень основных угроз безопасности сети (сетей) электросвязи

Перечень основных угроз безопасности сети (сетей) электросвязи должен соответствовать приведенному в модели угроз и нарушителя безопасности сети (сетей) электросвязи с ранжированием угроз по вероятности их возникновения.

6.2.3 Перечень уязвимостей объектов ИБ сети (сетей) электросвязи

По результатам инвентаризации элементов инфраструктуры сети (сетей) электросвязи представляется возможным построить информационно-логическую модель, иллюстрирующую технологию обработки, хранения и передачи информации с выделением вероятных точек уязвимости, каждой из которых необходимо дать полную характеристику.

6.2.4 Определение возможных каналов утечки информации и НСД к средствам связи

При определении возможных каналов утечки информации и НСД к средствам связи необходимо учитывать, что ВН на объекты ИБ могут осуществляться по внешним и внутренним линиям связи, с автоматизированных рабочих мест, по недекларированным каналам доступа и т.д.

Транзитные и незадействованные (воздушные, настенные, наружные и заложенные в канализацию) кабели, цепи и провода должны быть рассмотрены на предмет их использования как каналов утечки информации и НСД к средствам связи.

7 Рекомендации по ведению паспорта организации связи по информационной безопасности

7.1 Ответственным за ведение паспорта организации связи по ИБ назначается администратор ИБ. Корректировку паспорта проводят ежегодно. Изменения структуры сетевых связей вносят немедленно. Корректировку электронных приложений паспорта (карты сети) проводят по мере возникновения изменений, но не реже одного раза в месяц.

7.2 Дополнения и замечания в паспорт могут вноситься по мере развития и совершенствования СОИБ и появления новых данных в разделах документа.

7.3 Паспорт должен храниться у администратора ИБ организации связи. Доступ к электронным приложениям паспорта, кроме администратора ИБ, должен иметь руководитель организации и начальник службы ИБ.

7.4 Сведения ограниченного доступа, содержащие обобщенную информацию о СОИБ организации связи и представленные в форме документа (паспорта), должны иметь соответствующий гриф секретности.

Приложение А
(обязательное)

Пример формы паспорта организации связи по информационной безопасности

Утверждаю

Руководитель организации связи

_____

«____»_____200__ г.

Паспорт

_____

(наименование организации связи)

по информационной безопасности

Согласовано

_____

(начальник службы ИБ)

«____»_____200__ г.

Разработал

_____

_____

(наименование населенного пункта дислокации организации)

_____

(год разработки)

А.1 Общие сведения об организации связи

А.1.1 Наименование организации связи

(полное и сокращенное наименования)

А.1.2 Адрес организации связи

(юридический и фактический адрес организации)

А.1.3 Сведения о государственной регистрации

(орган регистрации, регистрационный номер, дата, форма собственности)

А.1.4 Контактные реквизиты

(телефон, телекс, факс, электронная почта и др.)

А.1.5 Основные виды деятельности

А.1.6 Наличие лицензий на основные виды деятельности

ФОИВ в области связи _____

ФСБ России _____

ФСТЭК России _____

(лицензии других организаций) _____

А.1.7 Категория сети связи по требованиям ИБ (защите от НСД) _____

А.2 Ситуационный план организации связи

(графическая схема расположения организации связи на местности, контролируемая зона, пункты физического доступа в организацию персонала и автотранспорта, окружающая среда организации с возможными источниками угроз безопасности, структура пожарной и охранной сигнализации, размещение трансформаторной подстанции, аварийное электропитание, с расчетным временем срабатывания, размещение заземлителей и т.п.)

А.3 Инфокоммуникационная структура сети (сетей) электросвязи организации связи

А.3.1 Информационные ресурсы, требующие защиты

- сведения об абонентах, базы данных;
- информация управления;
- внутренняя информация (топология сети, таблицы маршрутизации, файлы конфигурации телекоммуникационного оборудования);
- данные, передаваемые в сети электросвязи и содержащие информацию пользователей;
- программное обеспечение системы управления сетью электросвязи;
- программное обеспечение средств связи;
- данные о прохождении (задержки при прохождении), параметрах, загрузке (использовании), мониторинге каналов связи;
- обобщенные сведения о местах дислокации узлов связи и установленном сетевом оборудовании;
- проектная и нормативно-техническая документация, представленная в электронном виде);
- сведения, раскрывающие структуру используемых механизмов обеспечения безопасности (средств защиты) сети (сетей) электросвязи.

А.3.2 Инфраструктура сети (сетей) электросвязи

А.3.2.1 Структура сети (сетей) электросвязи

А.3.2.2 Основные средства связи, участвующие в процессе хранения, обработки и передачи информации/данных

Таблица А.1 — Перечень основных средств связи, входящих в состав сети связи организации связи и влияющих на обеспечение информационной безопасности

Тип, наименование основных средств связи	Предприятие-изготовитель	Учетный номер	Место установки	Примечание

А.3.2.3 Перечень вспомогательных средств связи организации связи

Таблица А.2 — Перечень вспомогательных средств связи, оказывающих влияние на обеспечение информационной безопасности

Тип, наименование вспомогательных средств связи	Учетный номер	Место установки	Примечание

А.3.2.4 Программное обеспечение (используемые операционные системы, сетевое и прикладное программное обеспечение, базы данных)

Таблица А.3 — Используемое программное обеспечение

Наименование ПО	Разработчик	Сведения о защите и проверке ПО	Место установки	Примечание

А.3.2.5 Используемые протоколы информационного обмена в сети (сетях) электросвязи, в том числе защищенные криптографические протоколы

А.3.2.6 Схема размещения основных средств связи

(показывается привязка к границам контролируемых зон)

А.4 Схема электропитания и заземления основных средств связи

(показывается привязка к границам контролируемых зон)

А.5 Сведения о величине сопротивления заземляющих устройств

(указываются значение сопротивления и дата измерения)

А.6 Перечень основных документов, регулирующих обеспечение информационной безопасности в организации связи

(конкретный состав и содержание основных документов по обеспечению ИБ организации связи определяется, исходя из специфики организации связи и в соответствии с положениями раздела 12 ГОСТ Р 53110)

А.7 Архитектура системы обеспечения информационной безопасности сети (сетей) электросвязи

(указывается принятая в организации связи архитектура СОИБ, определяющая специфику и взаимосвязь уровней и подсистем с основными процессами функционирования СМИБ (по ГОСТ Р ИСО/МЭК 27001), с системой управления сетью электросвязи и другими технологическими системами

А.8 Сведения о подготовке специалистов по вопросам информационной безопасности

[приводятся сведения об общей подготовке и переподготовке на специализированных курсах специалистов службы ИБ (кто, когда, какое учебное заведение/курсы закончил, продолжительность обучения, специализация, номер свидетельства об обучении]

А.9 Структура службы информационной безопасности организации (оператора) связи

(указываются основные структурные подразделения службы ИБ организации связи, ее подчиненность, основные функции)

А.10 Сведения о реализованных механизмах обеспечения безопасности и средствах защиты инфокоммуникационной структуры сети (сетей) электросвязи организации связи

Таблица А.4 — Перечень механизмов обеспечения безопасности (средств защиты)

Наименование и тип механизма обеспечения ИБ (средства защиты)	Производитель	Учетный номер	Сведения о сертификации	Место установки	Примечание

Примечание — В перечень включаются механизмы обеспечения ИБ и средства защиты сети электросвязи, относящиеся к классам механизмов обеспечения безопасности (средств защиты), определенным в подразделе 10.4 ГОСТ Р 53110.

А.11 Основные характеристики физической защиты объектов организации связи

(должны быть отражены основные организационно-технические вопросы обеспечения физической защиты объектов организации связи, перечислены основные средства, используемые для обеспечения физической безопасности организации связи)

А.12 Сведения о подтверждении соответствия сети электросвязи (аттестации) требованиям ИБ

(должен быть указан сертификационный центр или лаборатория, проводившие проверку соответствия, номер и дата акта проверки соответствия сети электросвязи требованиям ИБ)

А.13 Сведения о проведении контроля состояния информационной безопасности организации связи

Таблица А.5 — Результаты проверки состояния информационной безопасности

Дата проведения проверки	Наименование организации, проводившей проверку	Результаты проверки	Примечание

Примечания

1 Результаты контрольно-проверочных мероприятий должны оформляться документально в виде актов проверки и данных, вносимых в таблицу.

2 В таблицу вносят проверки, проводимые лицами из числа руководящего состава организации связи, специализированными организациями или представителями ФОИВ, уполномоченными в областях связи, обеспечения безопасности и технической защиты информации).

А.14 Лист регистрации изменений

(указываются даты внесения изменений и номера разделов паспорта, подвергшихся изменениям)

Приложение Б
(рекомендуемое)

Категории сетей электросвязи по защите от НСД, устанавливаемые актом о категорировании (см. приложение В)

Тип сетей	Категории сетей электросвязи в зависимости от категорий узлов связи по защищенности		
	I «высшая»	II «средняя»	III «низшая»
Сети фиксированной телефонной связи	Узлы связи сетей междугородной и международной телефонной связи, сетей зоновой телефонной связи, узлы связи сетей местной телефонной связи с числом портов более 10000, а также транзитные и оконечно-транзитные узлы связи сетей местной телефонной связи, которые соединяются с узлами обслуживания вызовов экстренных оперативных служб	Узлы связи сети местной телефонной связи с числом портов от 1024 до 10000, за исключением транзитных и оконечно-транзитных узлов связи, которые соединяются с узлами обслуживания вызовов экстренных оперативных служб	Узлы связи сети местной телефонной связи с числом портов до 1024
Сети подвижной радиосвязи, сети подвижной радиотелефонной связи, сети подвижной спутниковой радиосвязи	Узлы связи сети подвижной радиосвязи, узлы связи сети подвижной радиотелефонной связи, узлы связи в составе наземных станций сопряжения сети подвижной спутниковой радиосвязи	—	—
Сети передачи данных	Международные транзитные узлы связи	Транзитные узлы связи	Оконечные узлы связи, оконечно-транзитные узлы связи
Сети телеграфной связи	Международные узлы связи	Междугородние узлы связи	Зоновые узлы связи

Приложение В
(рекомендуемое)

Образец акта о категорировании сети электросвязи по требованиям информационной безопасности (защите от НСД)

Утверждаю

Руководитель организации связи

_____

«____»_____200__ г.

АКТ
категорирования сети электросвязи

_____
(наименование организации связи)

по требованиям информационной безопасности (защите от НСД)

Комиссия в составе:
председатель:
члены комиссии:
рассмотрев исходные данные и системный проект сети связи *(наименование организации связи)*, условия ее эксплуатации, взаимосвязь с окружающей средой, определяемое возможными угрозами безопасности и потенциальными воздействиями нарушителя безопасности, описанными в пояснительной записке, в соответствии с положением о добровольной оценке соответствия сетей электросвязи требованиям ИБ (защите от НСД), определяющими порядок категорирования сетей электросвязи, решила установить сети электросвязи *(наименование организации связи)* (номер категории) категорию по информационной безопасности (защите от НСД).

Приложение: пояснительная записка по определению категории сети электросвязи на ____ листах.

Председатель _____

Члены комиссии _____

_____

Приложение Г
(справочное)

Порядок составления карты сети

Г.1 Карта сети является электронным приложением паспорта организации связи по ИБ и представляет собой опись всего используемого и обслуживаемого аппаратного и ПО, в том числе и в присоединенных сетях электросвязи.

Г.2 Карта сети представляет собой эталонную информацию о сетевой архитектуре, которая должна периодически сравниваться с текущим состоянием сети и в случае санкционированного изменения расположения и конфигурации аппаратного и ПО также изменяться с тем, чтобы карта сети содержала самую последнюю и актуальную информацию.

Г.3 Информация по сетевой архитектуре должна храниться в базе данных организации связи, доступ к которой возможен только руководителю организации связи и начальнику службы ИБ или администратору ИБ (дежурному администратору ИБ).

Г.4 Опись всей сетевой архитектуры должна содержать:

- топологию средств связи, участвующих в процессе хранения, обработки и передачи информации (данных), с указанием их сетевых адресов;
- данные по размещению всех средств связи с обозначением номеров рабочих комнат, этажей, зданий и населенных пунктов;
- данные по кабелям связи, скоммутированным в организации связи (тип, структура, направление, протяженность, условия и время прокладки, их физическая защищенность);
- данные по образованным каналам связи (тип, используемый протокол передачи, конечный адрес);
- отдельно данные по радиоканалам, радиорелейным, тропосферным и спутниковым каналам связи;
- характеристики трафика (пиковые, минимальные и средние значения сетевой нагрузки), пропускная способность каналов связи;
- адресные таблицы, таблицы маршрутизации (по направлениям связи);
- используемые защищенные каналы связи (принципы построения, протоколы и средства защиты);
- данные о каналах удаленного доступа (с кем обеспечивается доступ, чем образован канал, наличие модемов, поддерживающие протоколы);
- признаки принадлежности портов коммуникационного оборудования различным сетевым сегментам (с выделением портов конфигурирования);
- список пользователей, права и привилегии их доступа, списки контроля доступа (атрибуты ИБ);
- перечень оборудования оконечных устройств и установленного на них ПО;
- указание на принадлежность сетевых сегментов подразделениям организации связи, данные о закреплении средств связи за обслуживающим персоналом.

Примечание — Карта сети может использоваться для построения графа сети, предназначенного для расчета характеристик устойчивости функционирования сети электросвязи, в соответствии с ГОСТ Р 53111.

Библиография

[1] Федеральный закон Российской Федерации № 126-ФЗ от 07.07.2003 «О связи»

[2] Требования по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации. Утверждены приказом министерства информационных технологий и связи Российской Федерации № 1 от 09.01.2008

УДК 351.864.1:004:006:354 ОКС 01.040.01 Т00

Ключевые слова: паспорт по информационной безопасности, сеть электросвязи, оператор связи, организация связи, система обеспечения информационной безопасности

Редактор *В.Н. Копысов*
Технический редактор *В.Н. Прусакова*
Корректор *М.В. Бучная*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 16.06.2009. Подписано в печать 30.07.2009. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 2,32. Уч.-изд. л. 1,40. Тираж 186 экз. Зак. 459.

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.