ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53110— 2008

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Общие положения

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Закрытым акционерным обществом «Компания ТрансТелеКом» (ЗАО «Компания ТТК»), Открытым акционерным обществом «Межрегиональный ТранзитТелеком» (ОАО «МТТ»), 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. № 528-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Май 2020 г.

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

© Стандартинформ, оформление, 2009, 2020

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

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины и определения 2
4 Сокращения 3
5 Цели и задачи обеспечения информационной безопасности 3
6 Взаимосвязь системы обеспечения информационной безопасности и системы менеджмента информационной безопасности 3
7 Жизненный цикл системы обеспечения информационной безопасности и его взаимосвязь с жизненным циклом сети связи 6
8 Направления обеспечения информационной безопасности 8
9 Подтверждение соответствия сетей электросвязи требованиям информационной безопасности . . 10
10 Архитектура системы обеспечения информационной безопасности 11
11 Система обеспечения информационной безопасности как технологическая система сети связи общего пользования 13
12 Документы, регулирующие обеспечение информационной безопасности в организации связи . . . 15
13 Служба информационной безопасности 17
Библиография 19

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Общие положения

Information security of the public communications network providing system.
General principles

Дата введения — 2009—10—01

1 Область применения

Настоящий стандарт определяет правовые, организационные и технические направления обеспечения информационной безопасности сетей электросвязи, входящих в состав сети связи общего пользования.

Настоящий стандарт распространяет положения по обеспечению безопасности сетей электросвязи, установленные ГОСТ Р 52448, на систему обеспечения информационной безопасности сети связи общего пользования, определяя ее как комплекс взаимодействующих систем обеспечения информационной безопасности сетей электросвязи, входящих в состав сети связи общего пользования.

Положения настоящего стандарта подлежат применению расположенными на территории Российской Федерации организациями, предприятиями и другими субъектами хозяйственной деятельности независимо от их организационно-правовой формы и формы собственности, имеющими лицензии федерального органа исполнительной власти, уполномоченного в области связи, на предоставление услуг связи.

Положения настоящего стандарта также распространяются на выделенные и технологические сети связи при их присоединении к сети связи общего пользования.

Настоящий стандарт устанавливает общий подход к:

- формированию и проведению в организации связи единой политики информационной безопасности сетей электросвязи;
- принятию управленческих решений по внедрению практических мер, реализующих организационные и функциональные требования безопасности;
- координации деятельности структурных подразделений организации связи при проведении работ по проектированию, построению, реконструкции и определяемых федеральными органами исполнительной власти, уполномоченными в областях связи, обеспечения безопасности и технической защиты информации.

Настоящий стандарт не конкретизирует:

- номенклатуру используемых механизмов обеспечения безопасности и средств защиты;
- требования по организации охраны сооружений и линий связи;
- обеспечение сохранности и физической целостности средств связи;
- защиту от стихийных бедствий и сбоев в системе энергоснабжения;
- меры по обеспечению личной безопасности сотрудников организации связи и пользователей услугами связи.

Настоящий стандарт не исключает возможности объединения процессов осуществления физической безопасности и функционирования системы обеспечения информационной безопасности организации связи в единую структуру.

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ Р 53109 Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности

ГОСТ Р ИСО/МЭК 17799 Информационная технология. Практические правила управления информационной безопасностью[1)]

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

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **информационная безопасность сети электросвязи:** Способность сети электросвязи противостоять преднамеренным и непреднамеренным дестабилизирующим воздействиям (угрозам безопасности) на входящие в состав сети средства и линии связи в процессе приема и передачи, обработки и хранения информации, что может привести к ухудшению качества услуг, предоставляемых сетью электросвязи.

3.2 **объект информационной безопасности сети электросвязи:** Элемент инфокоммуникационной структуры сети электросвязи (аппаратные, программные, программно-аппаратные средства, информационные ресурсы, услуги, процессы), над которым выполняются действия.

3.3 **субъект информационной безопасности сети электросвязи:** Лицо или инициируемые от его имени процессы по выполнению действий над объектами информационной безопасности сети электросвязи.

3.4 **мониторинг событий информационной безопасности сети электросвязи:** Постоянный контроль и действия по наблюдению, получению, хранению, распознанию и анализу информации, связанной с событиями информационной безопасности, выявлению фактов, признаков и причин нарушения установленных требований и объектов/субъектов, с которыми связаны эти нарушения.

3.5 **администратор системы обеспечения информационной безопасности сети электросвязи:** Субъект инфокоммуникационной структуры сети электросвязи, ответственный за выполнение процессов обеспечения информационной безопасности сети электросвязи.

3.6 **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.

3.7 **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.

[1)] Действует ГОСТ Р ИСО/МЭК 27002—2012.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ВН — воздействие нарушителя;
ИБ — информационная безопасность;
ИТ — информационная технология;
НПА — нормативно правовой акт;
НСД — несанкционированный доступ;
НТД — нормативно-технические документы;
ОРД — организационно-распорядительные документы;
ОС — операционная система,
ПДК по ИБ — постоянно действующая комиссия по ИБ;
РД — руководящий документ;
СВТ — средство вычислительной техники,
СКЗИ — средства криптографической защиты информации;
СМИБ — система менеджмента информационной безопасности;
СОИБ — система обеспечения информационной безопасности;
ССОП — сеть связи общего пользования;
ФОИВ — федеральный орган исполнительной власти;
ЧС — чрезвычайная ситуация;
ЭМ ВОС — эталонная модель взаимосвязи открытых систем.

5 Цели и задачи обеспечения информационной безопасности

5.1 Цели, задачи и принципы обеспечения ИБ сети (сетей) электросвязи организации связи должны соответствовать целям, задачам и основным принципам обеспечения безопасности сетей электросвязи по ГОСТ Р 52448.

5.2 Дополнительно к задачам по ГОСТ Р 52448 в организации связи должно предусматриваться выполнение следующих задач:

- создание, реализация, поддержка функционирования, осуществление мониторинга и совершенствование СОИБ на основе использования процессного подхода к управлению ИБ;
- анализ рисков ИБ, определение способов обработки рисков и мероприятий по их снижению;
- обеспечение изолированности средств связи, участвующих в управлении сетями электросвязи, от внешних сетей и рабочих станций, обслуживающего сеть персонала;
- обеспечение контролируемого доступа обслуживающего персонала к системе управления сетями электросвязи;
- обеспечение централизованной аутентификации обслуживающего сети персонала при их доступе к средствам связи;
- паспортизация организаций связи по требованиям к ИБ.

Примечание — Оператором связи могут быть уточнены цели и задачи обеспечения ИБ сетей электросвязи в зависимости от выполняемых организацией связи функций и ее деловых целей, но формулировка целей и задач должна быть независима от способов их реализации.

5.3 СОИБ должна создаваться операторами связи в каждой организации связи для осуществления мероприятий и действий по снижению потенциального ущерба от реализации угроз безопасности до приемлемого уровня за счет устранения уязвимостей в сетях и средствах связи или существенного затруднения использования этих уязвимостей нарушителями безопасности.

Областью действия СОИБ являются средства, сооружения и линии связи, а также обслуживающий их персонал организации связи. СОИБ сети (сетей) электросвязи должна осуществлять реализацию политики ИБ оператора связи.

6 Взаимосвязь системы обеспечения информационной безопасности и системы менеджмента информационной безопасности

6.1 Обеспечение ИБ является непрерывным процессом, осуществляемым СОИБ и взаимоувязывающим правовую, организационную и техническую деятельность, проводимую под непосредственным

управляющим воздействием руководящего состава организации связи, направленную на поддержание функционирования сетей электросвязи в условиях воздействия угроз безопасности.

Мероприятия и действия по обеспечению ИБ должны осуществляться в рамках применения процессной модели, определенной в ГОСТ Р ИСО/МЭК 27001, путем реализации процессов управления. Функцией, объединяющей процессы, обеспечения, управления и менеджмента, является руководство ИБ.

6.1.1 Руководство ИБ — это деятельность по установлению и поддержанию структуры управления и процессов, обеспечивающих гарантию того, что политика ИБ в организации связи направлена на достижение деловых целей организации и совместима с действующими федеральными законами РФ и нормативными правовыми актами ФОИВ, уполномоченными в областях связи, обеспечения безопасности и технической защиты информации.

Руководство ИБ определяет конкретные роли, обязанности и ответственность руководящего состава организации связи в области обеспечения ИБ и предоставляет службе ИБ, возглавляющей СОИБ, полномочия по управлению процессами СМИБ, так как в соответствии с [1] — процесс «обеспечение» предполагает определение «сил» и «средств», выполняющих функции безопасности (служб безопасности), на которые в организации связи возлагается выполнение мероприятий и осуществление деятельности по управлению и обеспечению ИБ. Взаимосвязь процессов руководства, обеспечения, управления и менеджмента показана на рисунке 1.

6.1.2 Управление — это совокупность целенаправленных действий, включающих оценку ситуации и состояния объектов управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование и внедрение мер обеспечения безопасности).

Мероприятия и действия, реализующие процесс управления, должны быть коррелированы с действиями, выполняемыми при менеджменте ИБ, и не должны повторять друг друга.



Рисунок 1 — Взаимосвязь процессов руководства, менеджмента, управления и обеспечения

6.1.3 Менеджмент ИБ — это часть общей системы менеджмента организации связи, основанная на управлении рисками организации связи при создании, реализации, функционировании, мониторинге и совершенствовании СОИБ.

СОИБ для СМИБ является организационной структурой и инструментарием по внедрению и поддержанию процессов СМИБ в стадиях жизненного цикла сетей связи.

6.2 Основными процессами СМИБ, показанными на рисунке 1 и определяющими функционирование СОИБ, являются:

- управление рисками;
- внутренний аудит;

- управление инцидентами;
- управление изменениями.

6.2.1 Управление рисками

В результате выполнения процесса «управление рисками» определяется структура СОИБ и уточняется состав ее подсистем.

«Управление рисками» позволяет установить баланс между эксплуатационными расходами и экономическими затратами на меры обеспечения безопасности и достигнуть более эффективного выполнения деловых целей организации связи, защиты сетей электросвязи и передаваемой посредством них информации.

Общий подход к процессу «управления рисками» приведен разделах 5.5—5.13 ГОСТ Р 52448—2005.

Под управлением рисками понимается оценка и уменьшение рисков, которые могут воздействовать на сети электросвязи.

Процесс оценки рисков, являющийся определяющим в «управлении рисками» и исходными предпосылками в котором выступают данные, полученные при разработке перечня угроз и уязвимостей для конкретной сети электросвязи, показан на рисунке 2.

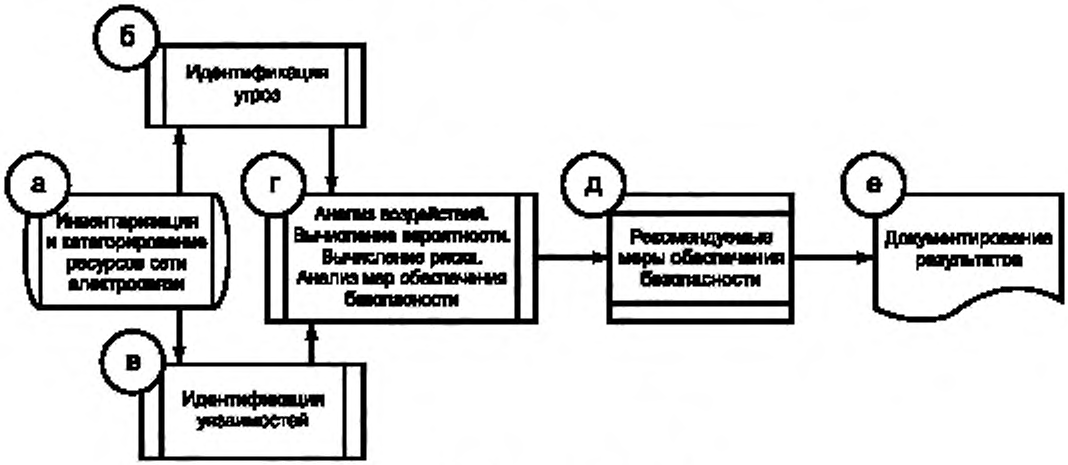

Рисунок 2 — Процесс оценки рисков

Процесс оценки рисков состоит из следующих этапов:

а) инвентаризация и категорирование ресурсов сети связи:

1) инвентаризация предполагает составление перечня всех ресурсов (активов), требующих защиты (информационные, программные, аппаратные и сервисные);

2) категорирование заключается в присвоении каждому ресурсу качественного или количественного параметра его значимости, с точки зрения его влияния на общее функционирование сети связи;

б) идентификация основных угроз;

в) идентификация уязвимостей.

Примечание — Процессы идентификации уязвимостей и угроз обычно осуществляются одновременно и служат основой для уточнения перечня угроз и уязвимостей;

г) анализ возможных воздействий угроз при реализации уязвимостей в ресурсах сети, вычисление вероятности этих воздействий и риска причинения ущерба сети, анализ существующих мер обеспечения безопасности;

д) определение дополнительных (рекомендуемых) мер обеспечения безопасности, способных противодействовать возможным воздействиям;

е) документирование полученных результатов.

Предлагается использовать качественный подход к анализу рисков, основанный на оценке влияния угроз и уязвимостей на основные критерии ИБ сети электросвязи (конфиденциальность, целостность, доступность и подотчетность). Анализ мер обеспечения безопасности и вычисление количествен-

ного значения риска относятся к основному процессу оценки риска и рассматриваются в отдельной методике.

6.2.2 Внутренний аудит

«Внутренний аудит» предназначен для получения объективных свидетельств соответствия действий участников процесса обеспечения ИБ требованиям СМИБ. В результате «внутреннего аудита» могут быть выявлены недостатки СОИБ, связанные с несоответствиями реализации предъявленных к СОИБ требований, ошибками при эксплуатации СОИБ, отсутствием необходимых ресурсов и т. д.

Сведения о выявленных недостатках должны учитываться в процессе «управления изменениями».

6.2.3 Управление инцидентами

«Управление инцидентами» предназначено для своевременного и всестороннего реагирования на инциденты ИБ. Реализация процесса «управление инцидентами» должна гарантировать, что инциденты ИБ будут корректно обрабатываться, а информация о событиях ИБ и уязвимостях, связанных с ресурсами сети электросвязи, — доводиться до сведения уполномоченных лиц в порядке, позволяющем вовремя предпринимать корректирующие действия.

Сведения о выявленных недостатках, способствующих появлению инцидентов ИБ, должны учитываться в процессе «управления изменениями».

6.2.4 Управления изменениями

«Управления изменениями» предназначено для выработки корректирующих действий, направленных на устранение причин выявленных несоответствий для предотвращения их повторного возникновения или корректирующих действий, связанных с предложениями по совершенствованию СОИБ. Полученные сведения о выявленных недостатках в процессе «управления инцидентами» и «внутреннем аудите» и информация, полученная в результате реализации процесса «управления рисками», являются исходными данными для выработки обобщенных предложений по совершенствованию функционирования СОИБ.

7 Жизненный цикл системы обеспечения информационной безопасности и его взаимосвязь с жизненным циклом сети связи

7.1 Жизненный цикл сети связи является полным процессом развития, реализации и вывода из эксплуатации сетей связи через процессы их проектирования, построения, реконструкции и эксплуатации.

Оператором связи могут быть применены различные методики для определения мероприятий и действий по обеспечению ИБ в процессе жизненного цикла сети связи, но каждая состоит из ряда определенных циклов или фаз, выполнение которых рекомендуется.

7.2 Для осуществления постоянного и корректного управления процессами менеджмента ИБ, СОИБ должна взаимодействовать с системой управления сетью связи и жизненный цикл СОИБ должен быть коррелирован с жизненным циклом сети связи и этапами процессной модели СМИБ, определенными в ГОСТ Р ИСО/МЭК 27001.

7.3 Настоящий стандарт устанавливает для жизненного цикла СОИБ следующие стадии:

- создание СОИБ;
- реализация СОИБ;
- функционирование СОИБ;
- мониторинг соответствия СОИБ;
- совершенствование СОИБ.

Взаимосвязь стадий жизненного цикла сети связи и СОИБ с этапами процессной модели СМИБ приведена на рисунке 3.

7.3.1 Стадия «создание системы обеспечения информационной безопасности»

При проектировании сети связи в разрабатываемом системном проекте [2], в отдельном разделе, должны быть описаны потребности ИБ, в частности:

- осуществлена предварительная классификация предполагаемых к использованию сетевых элементов и их категорирование с точки зрения их значимости в вопросах обеспечения ИБ;

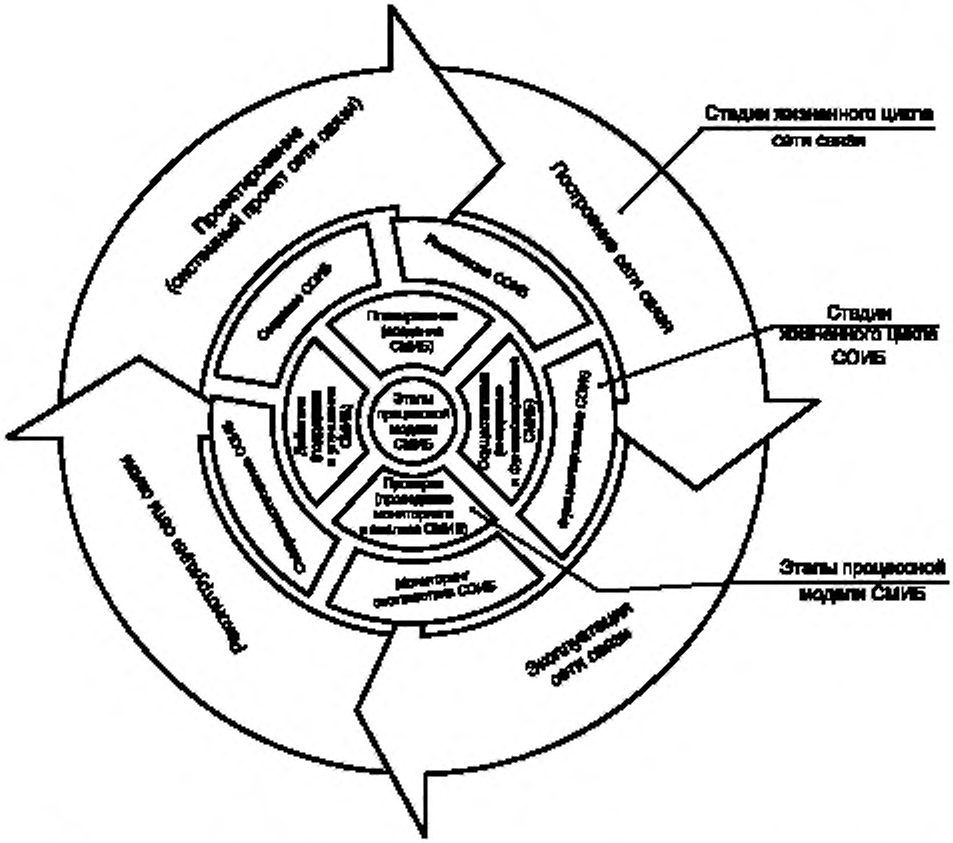

Рисунок 3 — Взаимосвязь стадий жизненных циклов сети связи и СОИБ с этапами процессной модели СМИБ

- определен предварительный перечень угроз и уязвимостей структурных элементов сети связи;
- проведена предварительная оценка рисков и на ее основе определены требования к ИБ и разработан перечень мер обеспечения ИБ, реализация которых должна определять использование конкретных механизмов обеспечения безопасности (средств защиты);
- определена предварительная структура СОИБ, состав подсистем и осуществляемые процессы ее функционирования, их взаимосвязь с процессами управления сетью и другими решаемыми сетью задачами.

7.3.2 Стадия «реализация системы обеспечения информационной безопасности»

При построении сети связи должны быть:

- реализованы результаты предварительной оценки рисков, выраженные в конструировании, разработке, закупке и внедрении необходимых средств обеспечения ИБ и средств защиты;
- сформирована функциональная структуру подсистем СОИБ;
- подготовлены необходимые для эксплуатации СОИБ документы;
- при возможности должна быть предварительно определена эффективность выбранных мер обеспечения безопасности.

7.3.3 Стадия «функционирование системы обеспечения информационной безопасности»

В процессе эксплуатации сети связи обеспечение ИБ должно быть интегрировано в процессы управления сетью связи. При эксплуатации сети связи должны выполняться процессы управления инцидентами, внутреннего аудита, управления изменениями и другие процессы, определенные в СМИБ. Реализация данных процессов позволит своевременно провести необходимое и обоснованное совершенствование СОИБ.

7.3.4 Стадия «мониторинг соответствия системы обеспечения информационной безопасности»

При эксплуатации сети связи и ее реконструкции (модернизации) должны проводиться следующие процессы:

- тестирование компонентов, свойств и функции ИБ сети связи;
- внутренний аудит;
- управление рисками (в полном объеме);
- обработка инцидентов и управление изменениями.

Новые или измененные компоненты ИБ должны тестироваться отдельно с тем, чтобы подтвердить, что они функционируют должным образом, а далее в операционном окружении для подтверждения, что их интеграция в сеть связи не нарушит качество услуг связи и/или функций безопасности. По результатам процесса мониторинга должны быть внесены обоснованные изменения в СОИБ.

7.3.5 Стадия «совершенствование системы обеспечения информационной безопасности»

Стадия «совершенствование СОИБ» (процесс управление изменениями) предусматривает проведение корректирующих и предупреждающих действий, направленных на устранение причин выявленных несоответствий при осуществлении процессов управления рисками, инцидентами и внутреннего аудита.

Применение корректирующих и предупреждающих действий, на основе оценки рисков, обуславливается возможностью внесения в аппаратные и программные средства новых уязвимостей при их модернизации (модификации).

Примечание — При прекращении функционирования сети связи (фаза снятия с эксплуатации), перед утилизацией, передачей аппаратных средств или сдачи в ремонт все информационные и вычислительные ресурсы, особенно базы данных, таблицы маршрутизации (и т. д.), должны быть проверены на отсутствие в них остаточной информации.

8 Направления обеспечения информационной безопасности

8.1 Правовое направление обеспечения информационной безопасности

8.1.1 Правовое направление обеспечения ИБ предусматривает создание и поддержание функционирования СОИБ в организации связи на основе реализации общеобязательных правовых норм по ИБ, осуществляемых в соответствии с положениями:

- федеральных законов РФ;
- указов и распоряжений Президента РФ;
- постановлений и распоряжений Правительства РФ;
- нормативных правовых актов (приказов, распоряжений) ФОИВ, уполномоченных в областях связи, обеспечения безопасности и технической защиты информации.

8.1.2 Правовое направление обеспечения ИБ основывается на концептуальных правовых основах ИБ, определяемых:

- основными направлениями государственной политики в области ИБ;
- основными правами и обязанностями государства, ФОИВ, субъектов Российской Федерации, организаций связи и граждан в области ИБ;
- основными правилами и процедурами обязательной сертификации средств защиты информации и правилами аттестации объектов информатизации по требованиям технической защиты конфиденциальной информации,
- основными правилами и процедурами лицензирования деятельности в областях сохранения государственной тайны и технической защиты конфиденциальной информации;
- видами и формами ответственности организаций связи и граждан за нарушение правовых и нормативных требований по ИБ.

8.1.3 Правовое направление обеспечения ИБ в организации связи реализуется через систему внутренних документов организации связи, классификация которых приведена в разделе 12.

8.2 Организационное направление обеспечения информационной безопасности

Организационное направление обеспечения ИБ включает в себя:

- регламентацию взаимоотношения субъектов ИБ на нормативно-правовой основе;

- разработку и выполнение программ обучения и повышения компетентности сотрудников организации связи в вопросах ИБ;
- реализацию мероприятий по обеспечению ИБ;
- выполнение организационных требований безопасности.

8.2.1 Регламентация взаимоотношений субъектов ИБ предполагает:

а) определение в должностных инструкциях обязанностей и ролей сотрудников организации связи по вопросам выполнения требований ИБ. Роль в организации связи представляет заранее определенную совокупность правил, устанавливающих допустимое взаимодействие между субъектами и объектами в организации связи.

Примечание — К субъектам относятся лица из числа руководства организации связи, ее сотрудники, пользователи услугами связи или инициируемые от их имени процессы по выполнению действий над объектами;

б) установление мер ответственности сотрудников организации связи за нарушение ИБ;

в) определение ограничений в деятельности сотрудников организации связи и конечных пользователей, определяемых факторами обеспечения ИБ и другими условиями.

8.2.2 Программа обучения сотрудников организации связи вопросам ИБ предназначается для персонала, имеющего в своих функциональных обязанностях положения, касающиеся выполнения требований ИБ, и предполагает необходимость специального обучения для этой категории сотрудников. Глубина этого обучения зависит от степени важности ИБ для организации и должна варьироваться согласно требованиям безопасности к выполняемой работе. Программа обучения сотрудников ИБ должна быть разработана так, чтобы охватить все потребности в мерах безопасности, относящихся к сетям электросвязи. В случае необходимости может быть использовано обучение на уровне специальных курсов.

В организации связи должен быть составлен список сотрудников, для которых необходимо специальное обучение ИБ и список должностей, на которых должны использоваться сотрудники, получившие специализированное обучение на курсах или имеющие высшее образование в области ИБ.

Необходимость специального обучения ИБ должна быть определена для текущих и запланированных задач, проектов и т. д. Каждый новый проект, со специальными требованиями к ИБ, должен сопровождаться соответствующей программой обучения, разработанной до начала проекта.

8.2.3 Программа повышения компетентности сотрудников организации связи в вопросах ИБ относится к каждому сотруднику организации и должна гарантировать, что персонал имеет достаточный уровень знаний об основах обеспечения ИБ.

8.2.4 Реализация мероприятий по обеспечению ИБ должна предусматривать:

а) регулирование функционирования службы ИБ (см. раздел 13);

б) издание приказов и распоряжений по обеспечению ИБ, основными из которых являются:

1) о создании ПДК по ИБ;

2) о назначении комиссии по категорированию, классификации и аттестации объектов связи и информационных систем по требованиям к ИБ;

3) о допуске сотрудников к работе со средствами связи;

4) о назначении администратора ИБ и лиц, ответственных за обеспечение ИБ в подразделениях организации связи;

в) ограничение доступа к техническому, программному и аппаратно-программному оборудованию, кроссам, распределительным щитам, незащищенным линиям и каналам связи для предупреждения несанкционированного доступа к ним;

г) осуществление физической и инженерно-технической защиты объектов организации связи;

д) планирование действий по управлению инцидентами ИБ;

е) планирование действий в ЧС;

ж) включение в должностные инструкции сотрудников организации связи обязательства о неразглашении и сохранности сведений ограниченного доступа;

и) оборудование служебных помещений сейфами, шкафами для хранения бумажных, магнитных носителей информации и др.

8.2.5 Выполнение организационных требований безопасности предполагает:

- определение и внедрение организационных мер обеспечения безопасности;
- выполнение организационных мер, осуществляемое через процедуры, определяющие мероприятия и порядок действий по их осуществлению, описание которых не является однозначным и в настоящем стандарте не рассматривается;
- контроль выполнения организационных мер безопасности.

8.3 Техническое направление обеспечения информационной безопасности

Техническое направление обеспечения ИБ включает в себя мероприятия и действия по:

а) выполнению функциональных требований безопасности, путем:

1) определения функциональных мер безопасности;

2) внедрения, осуществления эксплуатации и контроля за техническим обслуживанием механизмов обеспечения безопасности и средств защиты, реализующих меры обеспечения безопасности;

б) реализации разрешительной системы допуска обслуживающего персонала к работам, документам и информации управления средствами связи;

в) разграничению доступа обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации в подсистемах различного уровня и назначения;

г) учету активов, регистрации действий пользователей и обслуживающего персонала, контролю за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;

д) предотвращению атак и внедрения в средства связи и автоматизированные системы программ-вирусов и программных закладок;

е) применению СКЗИ (при необходимости) для защиты обрабатываемой информации.

Примечание — В настоящем стандарте не рассматривается порядок использования СКЗИ, который регламентируется ФОИВ, уполномоченным в области обеспечения безопасности;

ж) надежному хранение носителей информации, ключей (ключевой документации) и их обращению, исключающему хищение, подмену и уничтожение;

и) резервированию технических средств, баз данных и носителей информации;

к) оборудованию информационных систем, средств связи и СВТ устройствами защиты от сбоев электропитания и помех в линиях связи;

л) постоянному обновлению технических и программных средств защиты от несанкционированного доступа к средствам связи и антивирусных средств в соответствии с меняющейся окружающей обстановкой.

9 Подтверждение соответствия сетей электросвязи требованиям информационной безопасности

9.1 Подтверждение соответствия сетей электросвязи (аттестация) требованиям ИБ носит добровольный характер.

9.1.1 Добровольное подтверждение соответствия осуществляется по инициативе оператора связи в форме добровольной сертификации.

9.1.2 Добровольное подтверждение соответствия может осуществляться для установления соответствия сети электросвязи требованиям к ИБ национальным стандартам, стандартам организаций, сводам правил, системам добровольной сертификации.

9.2 Подтверждение соответствия предусматривает комплексную проверку (аттестационные испытания) сети электросвязи и обеспечивающей ее инфраструктуры — СОИБ положениям настоящего стандарта, в реальных условиях эксплуатации.

При аттестации сети электросвязи подтверждается ее соответствие требованиям безопасности, в том числе способность сети по:

- защите от НСД к ней и передаваемой посредством нее информации;
- противодействию влияния вредоносных программ на средства связи и информатизации;
- обнаружению и противодействию атакам на средства связи и информатизации;
- содержанию охраняемых и контролируемых зон.

Примечание — Конкретные требования безопасности сетей электросвязи могут быть изложены в НПА ФОИВ, уполномоченного в области связи.

9.3 Проверка соответствия сети электросвязи требованиям безопасности должна осуществляться специализированными сертификационными центрами или лабораториями по методикам, разработанным в системе добровольной сертификации ИБ сетей электросвязи.

10 Архитектура системы обеспечения информационной безопасности

10.1 Основные положения

СОИБ является неотъемлемой частью любой сети связи, и ее архитектура не зависит от технологий, используемых при построении сети связи. СОИБ является предупредительной системой в отличие от ответной модели, осуществляющей обработку события после его происхождения. Процессы СОИБ должны работать до того как случится непредвиденный инцидент безопасности.

Архитектура СОИБ ССОП должна быть многоуровневой и включать в себя следующие функциональные структурные элементы: уровни ИБ, подсистемы ИБ, службы обеспечения ИБ различных организаций (операторов) связи, координируемые центральным органом СОИБ ССОП, который может быть образован ФОИВ, уполномоченным в области связи.

10.2 Уровни системы обеспечения информационной безопасности

Архитектура СОИБ может содержать следующие уровни ИБ, описание которых приведено в разделе 8 ГОСТ Р 52448:

- управление ИБ;
- организационно-административный;
- безопасность инфокоммуникационной структуры;
- безопасность услуг;
- сетевая безопасность;
- физическая безопасность.

Оператор связи в целях обеспечения своей деятельности и достижения деловых целей может уточнять данные архитектурные компоненты, в частности, описанные уровни СОИБ, могут быть объединены в три укрупненных уровня:

- организационный;
- организационно-технический;
- технический.

10.3 Подсистемы системы обеспечения информационной безопасности

Разделение СОИБ на подсистемы носит условный характер и предназначено для объединения характерных мероприятий и действий по обеспечению ИБ в единую архитектурную компоненту. В общем случае в состав СОИБ могут входить следующие функциональные подсистемы:

- аутентификации и авторизации;
- контроля доступа и защиты от НСД;
- регистрации событий ИБ и аудита;
- управления;
- резервирования.

10.3.1 Подсистема «аутентификации и авторизации»

Подсистема «аутентификации и авторизации» предназначается для централизованной аутентификации и авторизации доступа субъектов к программно-аппаратным средствам связи и системе управления.

Основными функциями подсистемы «аутентификации и авторизации» являются:

- предоставление обслуживающему персоналу систем и сетей связи возможности использования одной (или нескольких) учетной записи и пароля при доступе к средствам связи и серверам системы управления с использованием механизмов внешней аутентификации и авторизации;
- централизованное хранение базы данных пользователей и их авторизационной информации с использованием механизмов внешней аутентификации и авторизации.

Подсистема «аутентификации и авторизации» может быть реализована встроенными механизмами аутентификации и авторизации средств связи и информатизации и является одним из звеньев получения доступа к средствам связи, реализующему следующие логические процессы:

- идентификацию пользователя, когда определяется имя учетной записи или логин;
- аутентификацию — проверку подлинности того, что предъявитель имени учетной записи является лицом, чью учетную запись он предъявил в процессе идентификации;
- авторизацию — процесс наделения правами доступа к оборудованию.

В подсистеме «аутентификации и авторизации» допускается применение аутентификации разных уровней сложности:

а) однофакторной аутентификации с использованием:
   1) пароля;
   2) пароля однократного действия;

б) двухфакторной аутентификации с использованием:
   1) токенов;
   2) смарткарт;
   3) криптокарт;
   4) сертификатов;

в) трехфакторной аутентификации с использованием биометрических методов.

10.3.2 Подсистема «контроля доступа и защиты от НСД»

Подсистема «контроля доступа и защиты от НСД» предназначена для:

- разделения передаваемого трафика пользователей и системы управления;
- обеспечения целостности маршрутной информации и информации о текущем времени;
- защиты управляющего трафика и компонентов СОИБ;
- разграничения доступа к системе управления сетью (сетями) электросвязи.

Подсистема «контроля доступа и защиты от НСД» реализуется посредством средств сегментирования сети, межсетевого экранирования, организации криптографических туннелей и антивирусного контроля.

10.3.3 Подсистема «регистрации событий ИБ и аудита»

Подсистема «регистрации событий ИБ и аудита» предназначена для:

- мониторинга сетевой активности и оповещения о событиях, связанных с ИБ на сетевом уровне;
- мониторинга активности системного уровня (уровень ОС) и оповещения о событиях, связанных с ИБ на системном уровне;
- консолидации информации об активности сетевого и системного уровня на централизованную консоль управления;
- ведения журналов аудита событий ИБ;
- регистрации действий персонала, управляющего средствами связи и компонентами СОИБ;
- автоматизированного контроля защищенности объектов ИБ сети (сетей) электросвязи и компонентов СОИБ с целью выявления уязвимостей;
- формирования отчетов по результатам анализа защищенности и рекомендаций по устранению выявленных уязвимостей;
- автоматизированного анализа журналов аудита.

Подсистема «регистрации событий ИБ и аудита» реализуется с использованием механизмов анализа журналов событий, анализа защищенности и обнаружения/предотвращения вторжений.

10.3.4 Подсистема «управления СОИБ»

Подсистема «управления СОИБ» предназначена для:

- организации безопасного удаленного доступа к системе управления сетью (сетями) электросвязи;
- осуществления централизованного управления и мониторинга компонентами СОИБ;
- организации безопасного удаленного доступа к средствам связи для управления в случае отказов, следствием которых является невозможность управления оборудованием по основной схеме через технологическую сеть;
- контроля выполнения требований НТД.

Подсистема «управления СОИБ» должна по возможности использовать штатные средства управления и мониторинга компонентов СОИБ.

10.3.5 Подсистема «резервирования»

Подсистема «резервирования» предназначается для:

- дублирования основных компонентов СОИБ;
- резервного копирования информации СОИБ и системы управления сетью электросвязи.

Подсистема «резервирования» СОИБ должна обеспечивать бесперебойную работу механизмов обеспечения безопасности и надежное сохранение файлов регистрации событий ИБ.

Подсистема «резервирования» реализуется:

- за счет встроенных механизмов обеспечения надежности средств обеспечения ИБ;

- на основании рекомендаций поставщиков механизмов обеспечения безопасности (средств защиты);
- средствами резервного копирования информации.

10.4 Механизмы обеспечения безопасности и средства защиты

10.4.1 Выполнение функций, определенных для каждой подсистемы СОИБ, осуществляется с использованием конкретных механизмов обеспечения безопасности и средств защиты, реализующих функциональные меры обеспечения безопасности, определенные требованиями безопасности сетей электросвязи.

10.4.2 По своему назначению и характеристикам механизмы обеспечения безопасности и средства защиты условно объединяются в классы, ориентировочный перечень которых с обозначением их использования в подсистемах СОИБ приведен в таблице 1.

Таблица 1 — Перечень классов механизмов обеспечения безопасности, средств защиты и их использование в подсистемах СОИБ

Наименование классов механизмов обеспечения безопасности и средств защиты	Подсистемы СОИБ				
	Аутентификации и авторизации	Контроля доступа и защиты от НСД	Регистрации событий ИБ и аудита	Управления	Резервирования
1 Межсетевого экранирования и сегментирования сетей		+			
2 Защиты от НСД		+			
3 Криптографической защиты информации (СКЗИ)	+	+			
4 Контроля доступа		+			
5 Аутентификации	+				
6 Обнаружения/предотвращения вторжений			+		
7 Резервного копирования и архивирования					+
8 Централизованного управления ИБ				+	
9 Аудита и мониторинга событий ИБ			+		
10 Контроля деятельности сотрудников в Интернет			+		
11 Анализа содержимого почтовых сообщений			+		
12 Контроля защищенности			+		
13 Защиты от спама		+			
14 Защиты от атак класса «отказ в обслуживании»			+		
15 Контроля целостности		+			
16 Антивирусной защиты		+			
17 Защиты от утечки по техническим каналам		+			

11 Система обеспечения информационной безопасности как технологическая система сети связи общего пользования

11.1 СОИБ является технологической системой ССОП наряду с другими технологическими системами (сигнализации, тактовой сетевой синхронизации, управления и административно-биллинговой). Взаимодействие СОИБ с этими системами приведено на рисунке 4.

11.2 Основными функциями СОИБ как технологической системы ССОП являются:

- внедрение и контроль выполнения требований нормативной правовой базы в области обеспечения ИБ ССОП;

- создание условий для реализации прав граждан и общественных объединений на деятельность в сфере информационного обмена;
- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
- оценка состояния ИБ ССОП, выявление источников внутренних и внешних угроз безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз.



Рисунок 4 — Взаимосвязь СОИБ с технологическими системами ССОП

11.3 Одной из задач СОИБ является обеспечение безопасности технологических систем и, прежде всего, системы управления сетью (сетями) электросвязи, для чего СОИБ должна:
- предусматривать надежную защиту всех типов инфокоммуникационных ресурсов сети (сетей) электросвязи;
- учитывать специфику новых ИТ и интеграцию технологий безопасности между ИТ и сетевыми элементами;
- использовать централизованное управление всеми механизмами обеспечения безопасности (средствами защиты) из единого центра;
- обеспечивать ИБ мерами, соответствующими степени возможного нанесения потенциального ущерба в случае ВН;
- использовать в составе СОИБ только сертифицированные механизмы обеспечения безопасности (средства защиты).

11.4 Взаимосвязи между СОИБ и другими технологическими системами ССОП, приведенные на рисунке 4, подразумевают наличие в каждой технологической системе ССОП элементов подсистем обеспечения ИБ. Основными функциями данных подсистем должны быть:

а) использование систем распределенного мониторинга и анализа общеканальной сигнализации № 7 в «системе сигнализации»;

б) недопущение несанкционированного вмешательства в работу «системы тактовой сетевой синхронизации»;

в) обеспечение изолированности и защищенности «системы управления» от внешних сетей связи и осуществление контроля над действиями в сети (сетях).

Основной целью обеспечения ИБ в условиях ВН на сетевые ресурсы «системы управления» является сохранение следующих основных критериев ИБ:
- конфиденциальность информации управления;
- целостность информации управления;
- доступность информации управления;
- подотчетность участников (субъектов) управления;

г) в системе «административно-биллинговой»:

- обеспечение безопасности персональных данных, сведений об абонентах и предоставляемых им услугах связи,
- разработка политики борьбы с мошенничеством как со стороны внешних злоумышленников, так и со стороны собственного персонала,
- развертывание на сети связи системы обнаружения мошенничества, направленной на защиту доходов оператора и мониторинг незапланированных потерь,
- мониторинг деятельности и событий, связанных со счетами клиентов и с оплатами счетов.

12 Документы, регулирующие обеспечение информационной безопасности в организации связи

12.1 Документы, регулирующие обеспечение ИБ в организации связи, представляют собой объединенную целевой направленностью упорядоченную совокупность требований, правил, процедур и инструкций на бумажных носителях и в электронном виде, определяющих и ограничивающих функциональность объектов и деятельность субъектов, принимающих участие в обеспечении ИБ.

12.2 Настоящий стандарт не определяет конкретного перечня документов, разрабатываемых в организации связи. Состав документов определяется исходя из деловых целей организации, используемых технологий и оборудования, структуры и объема предоставляемых услуг связи. Настоящий стандарт предлагает только целевую направленность разрабатываемых документов.

12.3 Документы, регулирующие ИБ в организации связи, разрабатываются с учетом положений общеобязательных правовых норм по ИБ (см. 8.1.1) и по своему функциональному назначению подразделяются на следующие основные классы:

- организационно-распорядительные;
- нормативно-технические;
- информационные.

Каждый из приведенных классов документов, в зависимости от характера и направленности изложения материалов, подразделяется на различные виды документов.

12.4 ОРД определяют и регламентируют деятельность по планированию и осуществлению процессов обеспечения ИБ в организации связи.

По характеру регламентируемых вопросов (решаемых задач) ОРД подразделяют на.

- организационные документы;
- распорядительные документы;
- документы подтверждения соответствия.

12.4.1 Организационные документы являются основополагающими документами в области обеспечения ИБ, они представляют:

- детализацию положений и требований правовых документов;
- систему взглядов и единый порядок обеспечения ИБ в организации связи;
- функциональность службы ИБ и ее взаимосвязь с другими структурными подразделениями организации связи;
- долговременные задачи, права, обязанности и меры ответственности в области обеспечения ИБ.

К основным, рекомендуемым, организационным документам по ИБ относятся:

- политика ИБ (концепция ИБ);
- паспорт организации связи по ИБ;
- план обеспечения ИБ организации связи;
- положения;
- инструкции.

12.4.1.1 Политика ИБ является долговременным документом и представляет документированную систему взглядов, определяющих цели и направления деятельности субъектов в области обеспечения ИБ.

Документ, представляющий политику ИБ организации связи, должен включать в себя общие положения, соответствующие требованиям, изложенным в ГОСТ Р ИСО/МЭК 17799.

12.4.1.2 Наряду с политикой ИБ в организации связи может быть разработана концепция ИБ. В данном случае в концепции ИБ излагаются вопросы, не нашедшие раскрытия в политике ИБ, и пер-

спективы совершенствования СОИБ, например, связанные с внедрением на сетях электросвязи новых технологий и расширения спектра предоставляемых пользователям услуг связи.

12.4.1.3 Паспорт организации связи по ИБ разрабатывается в соответствии с ГОСТ Р 53109.

12.4.1.4 План обеспечения ИБ организации связи представляет ежегодно формируемый координационный документ, определяющий действия, требуемые для реализации мероприятий по обеспечению ИБ в соответствии с политикой ИБ организации связи.

В плане обеспечения ИБ организации связи должно планироваться обеспечение всех систем, находящихся на эксплуатации в организации. При наличии выделенных систем или систем, требующих повышенного уровня безопасности возможна разработка отдельных планов обеспечения ИБ для таких систем.

12.4.1.5 Кроме основного плана ИБ в организации связи могут разрабатываться планы по реализации конкретных мероприятий обеспечения ИБ.

Примеры

1 План реагирования на инциденты безопасности.

2 План действий в ЧС.

3 План и схема обеспечения охраны организации связи.

12.4.1.6 Положения-документы, содержащие организационные указания по осуществлению конкретных направлений деятельности по обеспечению ИБ.

Примеры

1 Положение о службе ИБ.

2 Положение о ПДК по ИБ.

12.4.1.7 Инструкции — документы, содержащие указания и правила, устанавливающие порядок и способ выполнения или осуществления определенных действий.

Примеры

1 Инструкция по обеспечению антивирусной защиты.

2 Инструкция администратору ИБ.

12.4.2 Распорядительные документы — документы текущего управления, которые издаются во исполнение или в дополнение к организационным документам и устанавливают направления, методы (способы, приемы) организации работ по обеспечению ИБ в зависимости от возникающих конкретных задач управления и изменяющихся условий окружающей среды.

Основными видами распорядительных документов по ИБ являются приказы, программы, перечни, решения, распоряжения, указания.

12.4.3 К документам, подтверждающим соответствие продукции, работ и услуг в области ИБ, относятся:

а) документы вышестоящих регулирующих органов:

1) лицензии на право проведения работ со сведениями, составляющими государственную тайну;

2) лицензии на право осуществления работ в области технической защиты информации;

3) лицензии на право осуществления работ в области криптографической защиты информации;

4) сертификаты соответствия средств ЗИ;

б) внутренние документы организации связи.

Пример — Акт категорирования сети электросвязи по требованиям ИБ.

12.5 НТД устанавливают единые требования, нормы и правила обеспечения ИБ, обязательные для исполнения в пределах установленной при их введении сферы действия и области распространения.

12.6 Основными видами НТД являются:

- документы системы стандартизации Российской Федерации;
- РД ФОИВ, уполномоченного в области технической защиты информации;
- методики, методические указания, нормы и др. документы, разработанные ФОИВ, уполномоченными в областях связи, обеспечения безопасности и технической защиты информации;
- документы организации связи, развивающие требования вышестоящих регулирующих органов и положения внутренних ОРД организации связи.

12.7 К основным разрабатываемым в организации связи НТД относятся:

- стандарты организации связи;
- модель угроз и нарушителя ИБ сети электросвязи;
- руководства, процедуры, порядки, правила, рекомендации, перечни.

12.8 Информационные документы служат для информационной поддержки решения процессов обеспечения и осуществления ИБ.

По форме представления информационные документы могут быть следующих видов:

- справочные документы (справочные пособия, исходные данные для анализа активов организации связи, угроз, уязвимостей и др.);
- отчетная научно-техническая документация;
- научная и учебная литература;
- документы делопроизводства (акты, бланки, базы данных, донесения, журналы учета и др.).

12.9 НТД и информационные документы, разрабатываемые в организации связи, должны быть согласованы с руководителями заинтересованных подразделений организации связи и утверждены/подписаны руководителем службы ИБ организации связи.

12.10 Документация по обеспечению ИБ в организации связи должна периодически пересматриваться и обновляться по результатам оценки рисков, внешнего и внутреннего аудита ИБ, а также в связи с изменениями деловых целей и внедрения новых технологий и услуг связи.

13 Служба информационной безопасности

13.1 Создание СОИБ сети (сетей) электросвязи должно предусматривать формирование в организации связи организационно-штатной структуры (служба, отдел, подразделение, администратор ИБ), далее — служба ИБ организации связи, осуществляющей непосредственное выполнение мероприятий и действий по обеспечению ИБ сети электросвязи. Перечень основных выполняемых службой ИБ мероприятий приведен в подразделе 8.4 ГОСТ Р 52448—2005.

13.2 Организационно-правовой статус службы ИБ определяется:

- достаточной численностью службы ИБ для выполнения всех функций, определяемых настоящим стандартом;
- подчиненностью службы ИБ лицу, несущему персональную ответственность за обеспечение ИБ в организации связи;
- отсутствием у персонала службы других обязанностей, не связанных с обеспечением ИБ сети связи;
- профессиональной подготовкой сотрудников службы ИБ в области ИБ, подтвержденной дипломами и сертификатами;
- правом доступа сотрудников службы ИБ во все помещения, где установлены средства связи и информационные системы организации и правом прекращения обработки информации при наличии непосредственной угрозы для обрабатываемой информации;
- предоставлением права руководителю службы ИБ запрещать включение в число действующих новых элементов средств связи, если они не отвечают требованиям ИБ, что может привести к серьезным последствиям в случае реализации угроз ИБ;
- обеспечением условий для функционирования службы ИБ, необходимых для выполнения своих функций.

13.3 Для решения задач, возложенных на службу ИБ, ее сотрудники должны иметь следующие права:

- определять необходимость и разрабатывать документы, касающиеся вопросов обеспечения ИБ, включая документы, регламентирующие деятельность сотрудников других подразделений организации;
- получать информацию от сотрудников других подразделений организации по вопросам применения и эксплуатации средств связи и информационных систем;
- контролировать деятельность сотрудников других подразделений организации по вопросам обеспечения ИБ.

13.4 Структурно служба ИБ может иметь следующий состав:

- начальник службы ИБ;
- подразделение развития СОИБ (реализует процессы управления рисками и управление изменениями, внедрения средств обеспечения ИБ, участвует в процессе управление инцидентами);

- подразделение эксплуатации (реализует процесс эксплуатации средств обеспечения ИБ, управление инцидентами, участвует в процессе управления изменениями);

- подразделение аудита (реализует процесс внутреннего аудита, участвует в процессе управления изменениями).

13.5 В состав подразделений службы ИБ должны входить:

а) специалисты, способные администрировать,

1) средства защиты от НСД (выбор, установка, настройка, сопровождение, снятие средств защиты, просмотр журналов регистрации событий, оперативный контроль за работой пользователей и реагирование на события НСД и др.),

2) СКЗИ (выбор, учет, выдача, установка, настройка, сопровождение, снятие СКЗИ, генерация и распределение ключей, обучение пользователей правилам применения и др.),

3) средства сетевой безопасности и базы данных;

б) аналитики, способные участвовать:

1) в написании и экспертизе технической документации на сети связи (раздел системного проекта сети связи по ИБ),

2) в разработке технических требований по вопросам обеспечения ИБ,

3) в выборе методов и средств обеспечения ИБ (средств защиты),

4) в испытаниях новых прикладных программ с целью проверки выполнения требований по обеспечению ИБ и др.;

в) специалисты в области защищенных сетей связи и безопасности электронных АТС и др.

Библиография

[1] Федеральный закон Российской Федерации № 2446-1 от 5 марта 1992 г. «О безопасности»

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

УДК 351.864.1:004:006:354 ОКС 01.040.01

Ключевые слова: сеть электросвязи, оператор связи, организация связи, информационная безопасность, система обеспечения информационной безопасности

Редактор переиздания *Н.Е. Рагузина*
Технический редактор *И.Е. Черепкова*
Корректор *С.В. Смирнова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 25.05.2020. Подписано в печать 06.07.2020. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,40.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru