ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 52448— 2005

Защита информации

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТЕЙ ЭЛЕКТРОСВЯЗИ

Общие положения

Издание официальное

БЗ 12—2005/334

Москва
Стандартинформ
2006

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 Государственным научно-исследовательским испытательным институтом проблем технической защиты информации Федеральной службы по техническому и экспортному контролю (ГНИИИ ПТЗИ ФСТЭК России), Техническим комитетом по стандартизации ТК 362 «Защита информации»

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 29 декабря 2005 г. № 449-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

Защита информации

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТЕЙ ЭЛЕКТРОСВЯЗИ

Общие положения

Information protection.
Providing the security of networks telecommunications.
General provisions

Дата введения — 2007—01—01

1 Область применения

Настоящий стандарт предназначен для применения расположенными на территории Российской Федерации организациями, предприятиями и другими субъектами хозяйственной деятельности независимо от их организационно-правовой формы и формы собственности, которые связаны с созданием и эксплуатацией сетей электросвязи, являющимися составными компонентами сети связи общего пользования единой сети электросвязи Российской Федерации. Основными функциями сетей электросвязи являются прием, обработка, хранение, передача и предоставление требуемой информации пользователям и органам государственного управления для ее последующего применения. Сети электросвязи предназначены для оказания услуг связи любому пользователю путем предоставления открытых информационных ресурсов и информации, не содержащей сведений, составляющих государственную тайну, или информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

Настоящий стандарт определяет терминологию, цели, задачи, принципы и основные положения обеспечения безопасности сетей электросвязи.

Положениями настоящего стандарта рекомендуется руководствоваться при:

- развитии и совершенствовании правового, организационного, экономического и научно-технического обеспечения безопасности сетей электросвязи;
- разработке проектов, программ, нормативных документов и методических рекомендаций по обеспечению безопасности сетей электросвязи и контролю их состояния;
- формировании и реализации политики безопасности операторами связи.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 15408-2—2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК 15408-3—2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

ГОСТ Р 51275—99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального

Издание официальное

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 замененным (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:

Примечание — Взаимосвязь основных понятий и процессов обеспечения безопасности сетей электросвязи показана на примере «Модель безопасности сети электросвязи» (приложение А).

3.1 **безопасность сети электросвязи:** Способность сети электросвязи противодействовать определенному множеству угроз, преднамеренных или непреднамеренных дестабилизирующих воздействий на входящие в состав сети средства, линии связи и технологические процессы (протоколы), что может привести к ухудшению качества услуг, предоставляемых сетью электросвязи.

3.2 **дестабилизирующее воздействие:** Действие, источником которого является физический или технологический процесс внутреннего или внешнего по отношению к сети электросвязи характера, приводящее к выходу из строя элементов сети.

3.3 **инфокоммуникационная структура сети электросвязи:** Совокупность информационных ресурсов и инфраструктуры сети электросвязи.

3.4 **инфраструктура сети электросвязи:** Совокупность средств связи, линий связи, сооружений связи, технологических систем связи, технологий и организационных структур, обеспечивающих информационное взаимодействие компонентов сети электросвязи.

3.5 **информационные ресурсы сети электросвязи:** Совокупность хранимых (используемых для обеспечения процессов функционирования сети электросвязи), обрабатываемых и передаваемых данных, содержащих информацию пользователей и/или системы управления сетью электросвязи.

3.6 **устойчивость функционирования сети электросвязи:** Способность сети электросвязи выполнять свои функции при выходе из строя части элементов сети в результате дестабилизирующих воздействий.

3.7 **меры обеспечения безопасности:** Набор функций, определяющих возможности механизмов обеспечения безопасности сети электросвязи по непосредственной или косвенной реализации требований к безопасности.

3.8 **механизм обеспечения безопасности сети электросвязи:** Взаимоувязанная совокупность организационных, аппаратных, программных и программно-аппаратных средств, способов, методов, правил и процедур, используемых для реализации требований к безопасности сети электросвязи.

3.9 **нарушитель безопасности (нарушитель) сети электросвязи:** Физическое или юридическое лицо, преступная группа, процесс или событие, производящие преднамеренные или непреднамеренные воздействия на инфокоммуникационную структуру сети электросвязи, приводящие к нежелательным последствиям для интересов пользователей услугами связи, операторов связи и/или органов государственного управления.

3.10 **риск нарушения безопасности сети электросвязи:** Вероятность причинения ущерба сети электросвязи или ее компонентам вследствие того, что определенная угроза реализуется в результате наличия определенной уязвимости в сети электросвязи.

3.11 **система обеспечения безопасности ССОП:** Совокупность служб безопасности операторов сетей электросвязи ССОП и используемых ими механизмов обеспечения безопасности, взаимодействующая с органами управления сетями электросвязи, организация и функционирование которой осуществляется по нормам, правилам и обязательным требованиям, установленным в области связи.

3.12 **служба безопасности сети электросвязи:** Организационно-техническая структура оператора сети электросвязи, реализующая политику безопасности оператора связи и обеспечивающая функционирование системы обеспечения безопасности ССОП.

3.13 **угроза безопасности сети электросвязи:** Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба сети электросвязи или ее компонентам.

3.14 **уязвимость сети электросвязи:** Недостаток или слабое место в средстве связи, технологическом процессе (протоколе) обработки/передачи информации, мероприятиях и механизмах обеспечения безопасности сети электросвязи, позволяющие нарушителю совершать действия, приводящие к успешной реализации угрозы безопасности.

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

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

Примечание — Определение приведено в соответствии с Федеральным законом «О связи» [1].

3.17 **электросвязь:** Любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам.

Примечание — Определение приведено в соответствии с Федеральным законом «О связи» [1].

4 Сокращения

В настоящем стандарте используются следующие сокращения:

ИТ — информационная технология;
ВН — воздействие нарушителя;
СОБ — система обеспечения безопасности;
ССОП — сеть связи общего пользования;
НСД — несанкционированный доступ;
ОТБ — организационные требования безопасности;
ТТБ — технические требования безопасности;
ФТБ — функциональные требования безопасности;
ТДБ — требования доверия к безопасности;
НСВ — несанкционированные воздействия.

5 Основные положения по обеспечению безопасности сетей электросвязи

5.1 Сети электросвязи являются средой переноса сообщений любого рода в виде электрических сигналов. Сообщения содержат информацию пользователя, которая может быть открытой, закодированной, зашифрованной или скремблированной (что для сети электросвязи является неопределяющим), и служебную информацию (например, адрес получателя). Сеть электросвязи должна обеспечить целостность передаваемых сообщений и своевременность их доставки адресату.

Открытость сетей электросвязи не должна означать полную доступность ко всем ее информационным ресурсам и отсутствие контроля их использования. В сети электросвязи должна быть обеспечена защита собственной, служебной информации, предназначенной для управления работой сети или служб сети.

К информационным ресурсам сетей электросвязи, требующим защиты со стороны оператора связи, могут быть отнесены:

- сведения об абонентах, базы данных;
- информация управления;
- данные, содержащие информацию пользователей (обеспечение доступности и целостности);
- программное обеспечение систем управления сетями электросвязи;
- сведения о прохождении, параметрах, загрузке (использовании) линий связи магистральных сетей;
- обобщенные сведения о местах дислокации узлов связи и установленном сетевом оборудовании;
- сведения, раскрывающие структуру используемых механизмов обеспечения безопасности сети электросвязи.

5.2 Необходимость рассмотрения проблем обеспечения безопасности сетей электросвязи обусловлена:

- динамикой развития сетей электросвязи и их интеграцией с глобальными сетями связи, в том числе с Интернет;
- совершенствованием применяемых ИТ;
- ростом числа пользователей услугами связи и расширением спектра предоставления услуг связи;
- увеличением объемов хранимой и передаваемой информации;
- территориальной рассредоточенностью сложных информационно-телекоммуникационных структур;
- недостаточностью в сетях электросвязи необходимых механизмов обеспечения безопасности.

Эти проблемы существенно повышают уязвимость сетей, способствуют появлению новых угроз безопасности и определяют необходимость комплексного решения задач по обеспечению безопасности сетей электросвязи путем:

- организации эффективного, безопасного управления и взаимодействия сетей;
- поддержания гарантированных качественных характеристик процессов обработки информации в сетях электросвязи (качества обслуживания) в условиях возможных ВН на инфокоммуникационную структуру сетей электросвязи;
- создания в сетях электросвязи надежных и защищенных каналов по пропуску определенных категорий трафика, из совокупности которого могут быть извлечены сведения, способные нанести ущерб безопасности Российской Федерации;
- противодействия проявлению терроризма на сетях электросвязи, в том числе экстремистским действиям.

Решение данных проблем является функцией СОБ сетей электросвязи ССОП и служб безопасности операторов связи в рамках общих положений по безопасности сетей электросвязи, предлагаемых настоящим стандартом.

5.3 Основными целями обеспечения безопасности сетей электросвязи являются:

- достижение устойчивого функционирования и успешного выполнения заданных функций сетью электросвязи, в условиях возможного ВН, 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.

5.4 Основными задачами обеспечения безопасности сетей электросвязи являются:

- своевременное выявление, оценка и прогнозирование источников угроз безопасности, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития сетей электросвязи на всех уровнях иерархии единой сети электросвязи России (международном, междугороднем, зоновом, местном, на уровне пользования услугами связи и т. д.);
- выявление и устранение уязвимостей в средствах связи и сетях электросвязи;
- предотвращение, обнаружение угроз безопасности, пресечение их реализации и своевременная ликвидация последствий возможных ВН, в том числе и террористических действий;
- организация системы пропуска приоритетного трафика по сети электросвязи в случае чрезвычайных ситуаций, организация бесперебойной работы международной аварийной службы;
- совершенствование и стандартизация применяемых мер обеспечения безопасности сетей электросвязи.

Примечание — Операторами связи могут быть определены дополнительные цели и задачи обеспечения безопасности сетей электросвязи в зависимости от выполняемых организацией связи функций и ее бизнес-целей, но формулировка целей и задач должна быть независима от способов их реализации.

5.5 Оператор связи при осуществлении процесса управления функционированием сети электросвязи должен минимизировать возможные негативные ВН для обеспечения выполнения основных целей организации связи, в том числе и бизнес-процессов. Это достигается путем интегрирования в систему управления функционированием сети электросвязи процесса управления рисками.

На каждой стадии жизненного цикла сетей электросвязи (проектирование, строительство, реконструкция, развитие и эксплуатация) должна осуществляться деятельность по поддержанию управления рисками, основой которой являются процессы идентификации и оценки рисков.

Оценка риска при обеспечении безопасности сетей электросвязи должна производиться на основе анализа уязвимостей сетей электросвязи и угроз, способных реализовать эти уязвимости.

5.6 Угрозы могут способствовать причинению ущерба пользователям услугами связи, операторам и/или органам государственного управления.

За основу классификации угроз безопасности сетей электросвязи рекомендуется классификацию, установленную ГОСТ Р 51275, в соответствии с которой угрозы могут быть классифицированы:

- по природе возникновения: объективные (естественные) или субъективные (искусственные);
- по источнику возникновения: внешние или внутренние.

Источником угроз безопасности сетей электросвязи могут быть: субъект, материальный объект или физическое явление.

В процессе обеспечения безопасности сети электросвязи необходимо выявление всех возможных угроз инфокоммуникационной структуре сети.

Полное множество угроз безопасности не поддается формализации. Это связано с тем, что архитектура современных сетей электросвязи, используемые технологии обработки, хранения и передачи информации подвержены большому количеству объективных и субъективных дестабилизирующих воздействий. Но чем больше будет выявлено возможных угроз безопасности, тем точнее будет оценено состояние безопасности сети электросвязи.

К основным возможным угрозам безопасности сетей электросвязи могут быть отнесены следующие угрозы:

- уничтожение информации и/или других ресурсов;
- искажение или модификация информации;
- мошенничество;
- кража, утечка, потеря информации и/или других ресурсов;
- несанкционированный доступ;
- отказ в обслуживании.

Каждая выявленная угроза в соответствии с выбранной методикой оценки рисков должна ранжироваться по вероятности своего возникновения для последующего анализа рисков и оценки величины возможного ущерба сети электросвязи от реализации угроз. Пример трехуровневой градации вероятности возникновения угроз приведен в таблице 1.

Таблица 1 — Описание показателей вероятности возникновения угроз

Показатель вероятности возникновения угрозы	Описание действий нарушителя
Маловероятно	Нарушитель обладает очень незначительными техническими возможностями для реализации угрозы или мотивация для нарушителя очень низкая
Вероятно	Технические возможности, необходимые для реализации угрозы, не слишком высоки и разрешимы без большого усилия; кроме того, должно быть разумное побуждение для нарушителя, чтобы реализовать угрозу
Возможно	На сети электросвязи отсутствуют механизмы обеспечения безопасности, используемые для противодействия этой угрозе, и побуждение для нарушителя весьма высоко

5.7 В целях учета всех возможных сфер проявления угроз для каждой конкретной сети электросвязи необходимо разрабатывать модель угроз безопасности.

Модель угроз безопасности сети электросвязи представляет собой нормативный документ, которым должен руководствоваться заказчик при задании требований к безопасности сети, и разработчик, создающий эту сеть и службы обеспечения информационной безопасности сети при ее эксплуатации.

Модель угроз должна включать:

- описание ресурсов инфокоммуникационной структуры (объектов безопасности) сети электросвязи, требующих защиты;
- описание источников формирования дестабилизирующих воздействий и их потенциальных возможностей;
- стадии жизненного цикла сети электросвязи, в том числе определяющие ее технологический и эксплуатационный этапы;
- описание процесса возникновения угроз и путей их практической реализации.

В качестве приложения модель угроз безопасности должна содержать полный перечень угроз и базу данных о выявленных нарушениях безопасности сети электросвязи с описанием обстоятельств, связанных с обнаружением нарушений.

В соответствии с разработанной моделью угроз оценивается опасность угроз для каждой группы идентифицированных ресурсов инфокоммуникационной структуры сети электросвязи и услуг связи и определяются возможные меры обеспечения безопасности для противодействия каждой конкретной угрозе.

5.8 Угрозы безопасности сети электросвязи реализуются нарушителями безопасности через выявленные уязвимости инфокоммуникационной структуры сети, в которую они могут быть внесены на технологическом и/или эксплуатационном этапах ее жизненного цикла. Угрозы безопасности могут изменяться. Уязвимость может существовать на протяжении всего срока эксплуатации сети электросвязи или конкретного протокола, если она своевременно не устраняется разработчиком или по его представлению службами эксплуатации оператора связи.

5.9 Нарушителями безопасности сетей электросвязи могут быть:

- террористы и террористические организации;
- конкурирующие организации и структуры;
- спецслужбы иностранных государств и блоков государств;
- криминальные структуры;
- взломщики программных продуктов ИТ, использующихся в системах связи;
- бывшие сотрудники организаций связи;
- недобросовестные сотрудники и партнеры;
- пользователи услугами связи и др.

Основными мотивами нарушений безопасности сетей электросвязи могут быть:

- месть;
- достижение денежной выгоды, в том числе за счет продажи полученной информации;
- хулиганство и любопытство;
- профессиональное самоутверждение.

5.10 Для учета всех возможных ВН и определения его категории разрабатывается модель нарушителя безопасности сети электросвязи, под которой понимается абстрактное (формализованное или неформализованное) описание нарушителя политики безопасности.

Задача построения модели нарушителя безопасности сети электросвязи состоит в определении:

- штатных объектов и элементов сети, к которым возможен доступ;
- субъектов, допущенных к работе с оборудованием сети в период ее проектирования, разработки, развертывания и эксплуатации;
- перечня соответствия объектов доступа субъектам, которые могут быть потенциальными нарушителями.

При определении потенциального нарушителя и составлении его модели необходимо исходить из того, что нарушитель может быть как законным абонентом сети (принадлежать к персоналу, непосредственно работающему с абонентскими терминалами), так и посторонним лицом, пытающимся непосредственно или с помощью имеющихся у него технических и программных средств получить доступ к информационным ресурсам и инфраструктуре сети.

ВН, в основном, направлены на ухудшение качественных характеристик функционирования сетей электросвязи и могут осуществляться, как правило, путем поиска и использования эксплуатационных и технологических уязвимостей. ВН могут осуществляться:

- по каналам абонентского доступа, в том числе и беспроводным;
- по внутренним линиям связи;
- с рабочих мест систем управления и технического обслуживания;
- по недекларированным каналам доступа.

При этом могут использоваться как штатные, так и специальные средства связи.

5.11 ВН могут носить как непреднамеренный (случайный), так и преднамеренный характер.

Непреднамеренные (случайные) воздействия могут быть спровоцированы недостаточной надежностью средств связи, ошибками обслуживающего персонала, природными явлениями и другими объективными дестабилизирующими воздействиями.

Преднамеренные воздействия могут быть активными, пассивными и не преследующими целей.

5.11.1 Активные действия нарушителя предусматривают вмешательство в работу сети электросвязи, нарушение режимов ее функционирования и снижение качества обслуживания вплоть до полного прекращения предоставления услуг связи пользователям. Основные цели активных действий:

- подрыв репутации оператора-конкурента путем нарушения доступности услуг связи и/или ухудшения их характеристик;
- несанкционированное использование услуг.

5.11.2 Пассивные действия нарушителя предполагают нанесение вреда абоненту (пользователю услугами связи) путем использования выявленных уязвимостей сети электросвязи, но не наносящие прямого вреда сети электросвязи. Целью таких действий могут являться:

- перехват персональных данных пользователей (например, паролей для регистрации терминалов);
- перехват данных о финансовых сделках с целью нанесения ущерба бизнесу;
- наблюдение за выполняемым процессом (подготовка для новых атак — активных действий);
- поиск идеологических, политических выгод;
- шантаж, вымогательство.

5.11.3 Действия, не преследующие целей (хулиганство) — действия, не ставящие перед собой цели нанесения вреда конкретному физическому объекту или лицу.

5.12 Безопасность сети электросвязи характеризуется основными ее критериями:

- конфиденциальностью инфокоммуникационной структуры сети электросвязи;
- целостностью информации и услуг связи;
- доступностью информации и услуг связи;
- подотчетностью действий в сети.

5.12.1 Под конфиденциальностью инфокоммуникационной структуры сети электросвязи понимают свойство, позволяющее ограничить несанкционированный доступ к инфокоммуникационной структуре сети электросвязи и/или не раскрывать содержания информационных ресурсов сети неуполномоченным лицам, объектам или процессам.

Нарушение конфиденциальности — несанкционированное раскрытие информации управления, персональных данных пользователей и др.

5.12.2 Под целостностью информации и услуг связи понимают состояние сети электросвязи, при котором обеспечивается неизменность информации и доступность услуг связи для пользователей, независимо от преднамеренного или случайного несанкционированного ВН на инфокоммуникационную структуру сети, в том числе в чрезвычайных ситуациях.

Нарушение целостности — несанкционированная модификация или разрушение информационных ресурсов и инфраструктуры сети электросвязи.

5.12.3 Под доступностью информации и услуг понимается способность сети электросвязи обеспечить пользователям согласованные условия доступа к предоставляемым услугам связи и их получение, в том числе в условиях возможных ВН на инфокоммуникационную структуру сети электросвязи.

Нарушение доступности — нарушение доступа к использованию информации или услуг связи.

5.12.4 Под подотчетностью понимают свойство, которое обеспечивает однозначное отслеживание действий в сети любого объекта.

Нарушение подотчетности — отрицание действий в сети (например, участие в совершенном сеансе связи) или подделка (например, создание информации и претензии, которые якобы были получены от другого объекта или посланы другому объекту).

В таблице 2 показана взаимосвязь основных угроз и критериев безопасности сети электросвязи.

Таблица 2 — Отображение взаимосвязи основных угроз и критериев безопасности

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 2

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

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

- «низкое» потенциальное воздействие может привести к ограниченному неблагоприятному эффекту;
- «умеренное» потенциальное воздействие может привести к серьезному неблагоприятному эффекту;
- «высокое» потенциальное воздействие может привести к тяжелому или катастрофическому неблагоприятному эффекту.

В соответствии с используемой оператором связи методикой оценки рисков и с учетом вероятности возникновения угрозы и потенциального воздействия нарушителя по реализации данной угрозы должен определяться риск возможного нанесения ущерба сети электросвязи.

Величина риска может классифицироваться тремя показателями, приведенными в таблице 3.

Таблица 3 — Описание показателей величины возможного риска

Уровень значения показателя «величина риска»	Описание риска
Незначительный	Незначительные риски возникают, если атаки нарушителя на критические ресурсы являются маловероятными. Угрозы, причиняющие незначительные риски, не требуют противодействия. Риск считается допустимым
Существенный	Существенные риски для соответствующих ресурсов представлены угрозами, которые, вероятно, произойдут, даже если их воздействие является менее фатальным. Существенные риски должны быть минимизированы
Критический	Критические риски возникают, когда появляется угроза ущерба интересам оператора сети и когда не требуется больших усилий потенциальному нарушителю, чтобы навредить этим интересам. Критические риски должны быть минимизированы с самым высоким приоритетом

5.14 Обеспечение безопасности сетей электросвязи в условиях ВН должно осуществляться с учетом следующих основных принципов:

5.14.1 Комплексности использования всей совокупности нормативных правовых актов, организационных и режимных мер, аппаратных, программных и программно-аппаратных методов защиты, обеспечивающих безопасное функционирование сетей электросвязи.

5.14.2 Защищенности сбалансированных интересов пользователей, операторов связи и органов государственного управления.

Интересы пользователей состоят в доверии к сети и предлагаемым услугам связи, в том числе доступности услуг (особенно экстренного обслуживания) в случае катастроф, включая террористические акты.

Интересы операторов связи заключаются в выполнении ими своих обязательств перед пользователями услугами связи и защите от посягательств на свои финансовые и деловые интересы.

Интересы органов государственного управления определяются необходимостью предъявления требований к безопасности сетей электросвязи, обеспечения соблюдения операторами связи предъявляемых им требований к безопасности, добросовестной конкуренции и защиты персональных данных пользователей.

5.14.3 Управляемости методами, действиями и процедурами по обеспечению безопасности сетей электросвязи и контролю качества процессов передачи информации в условиях возможных ВН на инфокоммуникационную структуру сетей в соответствии с функциями системы управления сетью.

5.14.4 Непрерывности совершенствования методов, действий и процедур по обеспечению безопасности сетей электросвязи с учетом достигнутого отечественного и зарубежного опыта в условиях возможных ВН и изменения методов и средств этих воздействий.

5.14.5 Совместимости аппаратно-программных средств и технологий, применяемых в СОБ.

6 Общие требования к безопасности сетей электросвязи

6.1 На всех этапах проектирования, строительства, реконструкции, развития и эксплуатации сетей электросвязи и сооружений связи к ним должны предъявляться требования по обеспечению безопасного их функционирования, сопоставимые с возможными ВН на инфокоммуникационную структуру сетей электросвязи и ожидаемым ущербом от данных воздействий.

6.2 Требования к безопасности сетей электросвязи устанавливают федеральные органы исполнительной власти в области связи на основании законодательства в области связи и защиты информации, с учетом рекомендаций международных организаций по стандартизации, а также предложений отечественных саморегулируемых организаций в области электросвязи и лучшей практики отечественных операторов связи.

Требования по обеспечению безопасности конкретной сети электросвязи должны формироваться с учетом целей, функций и задач решаемых оператором связи, условий использования сети электросвязи в общей системе связи государства, специфики используемой технологии передачи информации, потенциальных угроз безопасности и возможных ВН, реальных проектных и эксплуатационных ресурсов и существующих ограничений на функционирование сети электросвязи, а также требований и условий взаимодействия с другими сетями электросвязи.

Предоставление и использование услуг и механизмов обеспечения безопасности может быть довольно дорогим относительно потерь при нарушении безопасности сетей электросвязи. Поэтому должно анализироваться соотношение между стоимостью мер по обеспечению безопасности и возможными финансовыми последствиями нарушения безопасности, при этом важно определить конкретные требования к безопасности в соответствии с услугами, подлежащими защите.

Требования по обеспечению безопасности сетей электросвязи включают:

- организационные требования безопасности;
- технические требования безопасности;
- функциональные требования безопасности;
- требования доверия к безопасности.

ОТБ содержат общие организационные, административные положения и процедуры по осуществлению мероприятий политики безопасности оператором связи.

ТТБ определяют требования к электропитанию, заземлению, к конструкции средств связи, к линейно-кабельным сооружениям связи, к прокладке линий связи и др., влияющие на обеспечение безопасности и устойчивости функционирования сетей электросвязи.

ФТБ и ТДБ содержат требования, определенные ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3 соответственно, которые для сетей и средств связи излагаются в профилях защиты и заданиях по безопасности и должны реализовываться на всех этапах жизненного цикла сетей электросвязи.

7 Основные мероприятия по обеспечению безопасности сетей электросвязи

7.1 Обеспечение безопасности сети электросвязи является обязанностью ее владельца. Ответственность владельца сети электросвязи за обеспечение ее безопасности не прекращается при делегировании им своих полномочий по данным функциям отдельным лицам (поставщикам услуг, администраторам, третьим лицам и т. д.).

Мероприятия по обеспечению безопасности сети электросвязи, проводимые оператором связи, не должны ухудшать качественных характеристик сети и снижать оперативность обработки информации.

Реализация обязательных требований к безопасности, установленных федеральными органами исполнительной власти в области связи, осуществляется силами и средствами владельца сети электросвязи с привлечением при необходимости специализированных организаций, имеющих лицензии на данный вид деятельности.

Дополнительные (повышенные) требования к безопасности (например, шифрование трафика пользователя) могут осуществляться оператором связи на договорной основе с пользователем.

Вопросы непосредственного обеспечения безопасности при присоединении одной сети электросвязи к другой и условия выполнения обязательных требований к безопасности, установленные федеральными органами исполнительной власти в области связи, при взаимодействии этих сетей оговариваются в заключаемых операторами связи договорах о присоединении сетей электросвязи.

При присоединении к сетям электросвязи иностранных государств и взаимодействии с глобальными информационно-телекоммуникационными сетями, в том числе и Интернет, обеспечение безопасности должно основываться на соблюдении международных правовых актов, регламентирующих безопасный пропуск трансграничного трафика. При этом должна быть обеспечена защита инфокоммуникационной структуры сетей электросвязи от НСД со стороны взаимодействующих сетей и гарантированное качество обслуживания в условиях возможных ВН трансграничного характера.

7.2 Обеспечение безопасности сетей электросвязи достигается:

а) защитой сетей электросвязи от НСД к ним и передаваемой посредством их информации;

б) противодействием техническим разведкам;

в) противодействием сетевым атакам и вирусам;

г) защитой средств связи и сооружений связи от НСВ, включая физическую защиту сооружений и линий связи;

д) разграничением доступа пользователей и субъектов инфокоммуникационной структуры сетей электросвязи к информационным ресурсам в соответствии с принятой политикой безопасности оператора связи;

е) использованием механизмов обеспечения безопасности;

ж) физической и инженерно-технической защитой объектов инфокоммуникационной структуры сетей электросвязи;

и) использованием организационных методов, включающих:

1) разработку и реализацию политики безопасности оператором связи;

2) организацию контроля состояния безопасности сети электросвязи;

3) определение порядка действий в чрезвычайных ситуациях и в условиях чрезвычайного положения;

4) определения порядка реагирования на инциденты безопасности;

5) разработку программ повышения информированности персонала сети электросвязи в вопросах понимания им проблем безопасности;

6) определение системы подготовки и повышения квалификации специалистов в области безопасности.

7.3 Пользователи услугами связи имеют право применять специальные механизмы обеспечения безопасности и средства защиты информации, разрешенные к применению на сетях электросвязи и сертифицированные в соответствии с действующим законодательством Российской Федерации.

Взаимоотношения пользователей с операторами связи в сфере обеспечения безопасности сетей электросвязи должны строиться на основе следующих положений:

- только авторизованные пользователи должны иметь доступ к сетям электросвязи и использованию предоставляемых им услуг;

- авторизованные пользователи должны иметь доступ и оперировать только теми ресурсами, к которым они допущены;

- все пользователи должны быть ответственными за их собственные, и только их собственные, действия в сети электросвязи.

7.4 Оператор связи должен принимать меры, обеспечивающие:

- доступ правоохранительных органов, в предусмотренных законодательством Российской Федерации случаях, к информации конкретных пользователей;

- право на доступ пользователей услугами связи к информационным ресурсам в строгом соответствии с установленными правилами разграничения доступа;

- исключение несанкционированного доступа пользователей услугами связи к ресурсам сети и услугам связи;

- предоставление пользователям услугами связи дополнительных услуг по защите информации и процесса безопасной передачи сообщений на договорной основе;

- информирование пользователей о состоянии безопасности доступа к услугам связи.

8 Основные положения о структуре системы обеспечения безопасности сетей электросвязи

8.1 Система обеспечения безопасности (СОБ) сетей электросвязи ССОП является элементом системы информационной безопасности Российской Федерации и может быть отнесена к категории технологических систем связи.

Архитектура СОБ сетей электросвязи имеет многоуровневую иерархическую структуру, охватывающую магистральные транзитные, междугородние и зоновые (местные и внутризоновые) сети электросвязи, и состоит из взаимодействующих между собой служб обеспечения безопасности различных операторов связи, координируемых центральным органом СОБ, который может быть образован федеральным органом исполнительной власти в области связи.

8.2 Архитектура СОБ сети электросвязи может состоять из нескольких уровней безопасности, характеристика которых должна быть отражена в политике безопасности организации связи. В общем случае архитектура СОБ может содержать следующие уровни безопасности:

а) уровень управления безопасностью. На данном уровне осуществляется управление безопасностью сетей электросвязи, координируемое центральным органом СОБ;

б) организационно-административный уровень. Включает службы (отделы, подразделения, администраторов) безопасности, в зависимости от структуры организации связи. На данном уровне осуществляются:

1) взаимодействие с системой управления сетями электросвязи;

2) управление, координация и контроль проводимых организационных и технических мероприятий на всех нижележащих уровнях;

3) учет практического применения нормативной правовой базы (законов, стандартов, положений, должностных инструкций, планов по безопасности);

в) уровень безопасности инфокоммуникационной структуры. Содержит механизмы обеспечения безопасности и другие средства, обеспечивающие защиту процесса обработки и передачи информации в сети. На данном уровне осуществляются:

1) разграничение доступа к информационным ресурсам, сетевым объектам и системе управления сетью электросвязи,

2) защита от НСД, аутентификация и идентификация участников сетевого взаимодействия, включая удаленные объекты и администраторов (сетевых и безопасности),

3) контроль трафика (межсетевые экраны), средства обнаружения атак, средства регистрации и учета событий и ресурсов (аудит и мониторинг безопасности);

г) уровень безопасности услуг. На данном уровне осуществляется контроль качества обслуживания (предоставляемых услуг связи) в условиях возможных ВН и в чрезвычайных ситуациях, в том числе целостности циркулирующих в сети сообщений, содержащих данные пользователя и информацию управления;

д) уровень сетевой безопасности. Данный уровень поддерживает безопасность сетевых протоколов, которые обеспечивают:

1) передачи трафика из конца в конец,

2) транспортирование файлов,
3) поддержку фундаментальных приложений, передачу голоса в сети и электронную почту;
4) конфиденциальность передаваемой по каналам связи информации управления;

е) уровень физической безопасности. На данном уровне обеспечиваются:
1) физическая охрана помещений, в которых обрабатывается и хранится информация,
2) организация контроля доступа сотрудников и посетителей на территорию организации связи, в помещения со средствами связи, осуществляющими обработку информации, к технологическим системам управления, кабельным соединениям,
3) организация охранной сигнализации,
4) контроль вскрытия аппаратуры,
5) электро- и пожаробезопасность организации связи в целом.

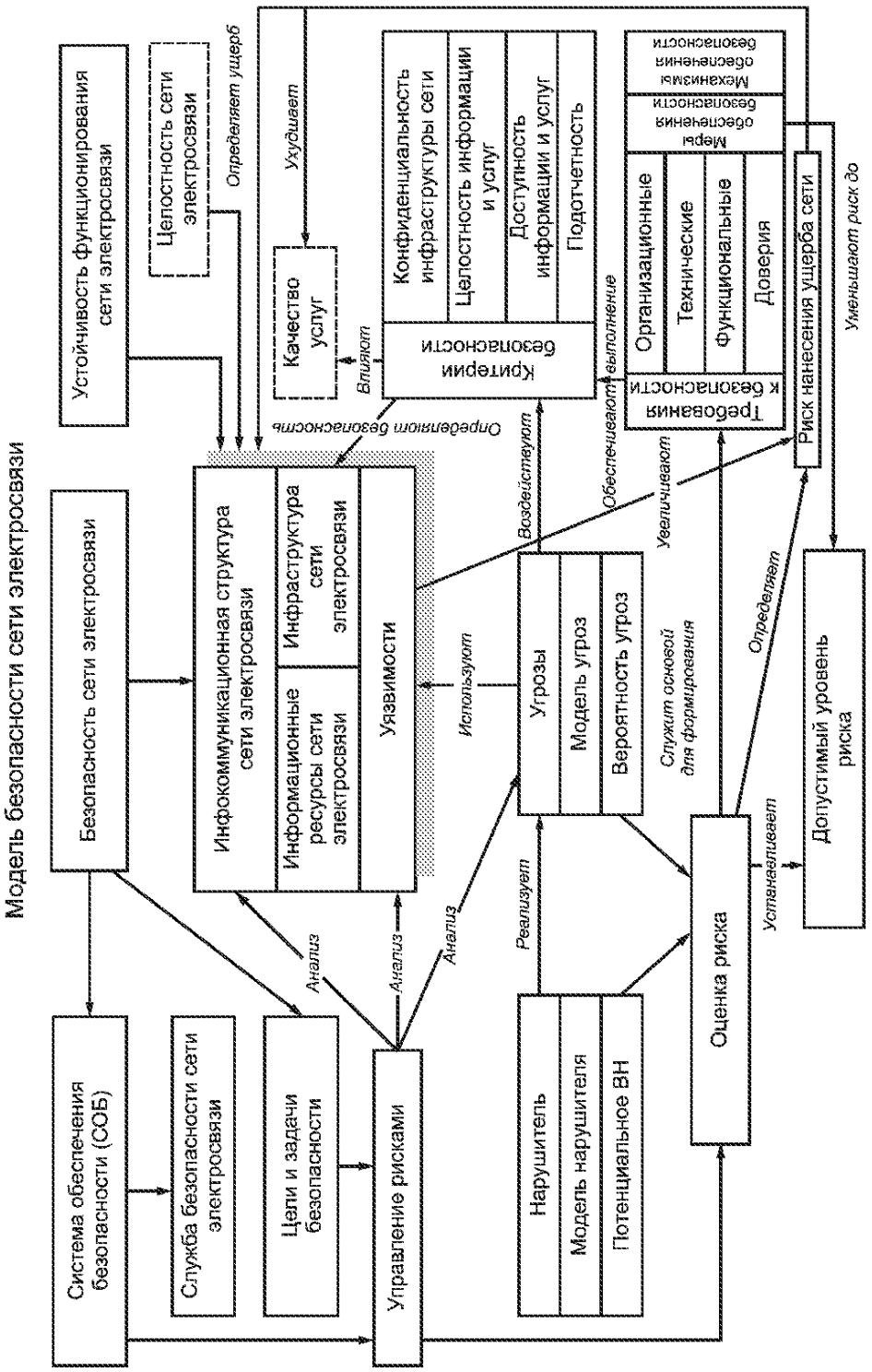
Оператор связи в целях обеспечения своей деловой деятельности и достижения бизнес-целей может определить дополнительные архитектурные компоненты СОБ.

8.3 Процедура создания СОБ сети электросвязи должна предусматривать формирование организационно-штатной структуры (отдел, подразделение, администратор безопасности) для непосредственного проведения мероприятий безопасности сети электросвязи.

8.4 Деятельность органов СОБ сети электросвязи подразумевает выполнение следующих мероприятий:

- подтверждение соответствия средств связи, паспортизацию организаций связи и аттестацию объектов и сетей электросвязи по требованиям безопасности;
- оценку состояния безопасности сети электросвязи, прогнозирование и обнаружение внутренних и внешних угроз безопасности;
- анализ информационных рисков, создание системы управления рисками и страхования информационных рисков;
- выявление уязвимостей в сетях электросвязи и осуществление комплекса адекватных и экономически обоснованных мер по их снижению;
- предотвращение либо обнаружение ВН, пресечение их реализации, локализацию и ликвидацию последствий этих дестабилизирующих воздействий на инфокоммуникационную структуру сети электросвязи;
- оповещение о нарушениях безопасности, реакцию на инциденты безопасности и восстановление нарушенного процесса функционирования сети электросвязи;
- адаптацию СОБ к изменяющимся условиям функционирования сети электросвязи;
- контроль качества обслуживания в условиях ВН;
- мониторинг СОБ и аудит событий безопасности;
- предупреждение, выявление и пресечение в сетях связи неправомочных действий пользователей услугами связи (нарушителей);
- противодействие распространению вредоносных программ (вирусов);
- организацию и проведение работ в области стандартизации безопасности сетей электросвязи с учетом рекомендаций и стандартов международных организаций по стандартизации;
- реализацию мер обеспечения безопасности сетей электросвязи, основой которых является применение соответствующих механизмов обеспечения безопасности.

Приложение А
(рекомендуемое)



Библиография

[1] Федеральный закон Российской Федерации № 126-ФЗ от 7.07.2003 г. «О связи»

УДК 001.4:025.4:006.354 ОКС 01.040.01 Т00

Ключевые слова: сеть электросвязи, безопасность, инфокоммуникационная структура, оператор связи, пользователь услугами связи

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *М.С. Кабашова*
Компьютерная верстка *В.И. Грищенко*

Сдано в набор 23.05.2006. Подписано в печать 03.07.2006. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 2,32. Уч.-изд. л. 1,75. Тираж 330 экз. Зак. 440. С 3010.

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