МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Российский государственный университет инновационных технологий и предпринимательства. Пензенский филиал»

В. М. Алексеев, Ю. Ю. Горюнов, А. П. Иванов

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ И СЕТЕЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Учебное пособие

Пенза
2012

УДК 004.056

Р е ц е н з е н т ы:
кандидат педагогических наук, доцент
кафедры «Прикладная математика и информатика»
Пензенского государственного педагогического университета
имени В.Г. Белинского
М.В. Баканова

Алексеев В. М., Горюнов Ю.Ю., Иванов А.П.

Обеспечение информационной безопасности систем и сетей передачи информации. – Пенза : Пенз. филиал РГУИТП, 2012. – 105 с. : ил.

Рассматриваются вопросы обеспечения безопасности систем передачи информации и используемых в них информационных технологий, а также сетей электросвязи в которых используются многоканальные системы. Излагаются сведения об основных положениях по построению систем менеджмента информационной безопасности в организациях электросвязи.

Учебное пособие подготовлено на кафедре «Информационные системы» и предназначено для студентов, изучающих дисциплины «Информационная безопасность» и «Многоканальные системы передачи и средства их защиты».

Введение

В настоящее время в мире складывается тенденция учета специфики объектов защиты при решении вопросов обеспечения информационной безопасности. Это характерно, в частности для телекоммуникационных систем и сетей.

Так, например, в нашей стране имеются попытки стандартизовать положения к обеспечению безопасности сетей электросвязи на основе современных риск-ориентированных подходов и использовании общих критериев оценки безопасности информационных технологий. В международном масштабе вопросами управления безопасности сетей занимается Международная организация по стандартизации, а Международный союз электросвязи адаптирует применительно к организациям электросвязи требования международных стандартов в виде своих рекомендаций.

Знание этих тенденций и основных положений и рекомендаций в области обеспечения безопасности телекоммуникационных систем и сетей весьма необходимо для развития компетенций будущих специалистов по защите информации, чем и объясняется актуальность данного учебного пособия.

1 Обеспечение безопасности сетей электросвязи

1.1 Общие положения и терминология

Основными функциями сетей электросвязи (СЭС), являющимися составными компонентами сети связи общего пользования единой сети электросвязи Российской Федерации, 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.

Под *безопасностью сети электросвязи* понимается способность СЭС противодействовать определенному множеству угроз, преднамеренных или непреднамеренных дестабилизирующих воздействий на входящие в состав сетей средства, линии связи и технологические процессы (протоколы), что может привести к ухудшению качества услуг,

предоставляемых СЭС. *Дестабилизирующими воздействиями* являются действия, источником которых являются физические и технологические процессы внутреннего или внешнего по отношению к СЭС характера, приводящие к выходу из строя элементов сети.

Под *инфокоммуникационной структурой сети электросвязи* понимается совокупность информационных ресурсов и инфраструктуры СЭС. *Инфраструктура сети электросвязи* определяется как совокупность средств связи, линий связи, сооружений связи, технологических систем связи, технологий и организационных структур, обеспечивающих информационное взаимодействие компонентов СЭС. *Информационные ресурсы сети электросвязи* - это совокупность хранимых (используемых для обеспечения процессов функционирования СЭС), обрабатываемых и передаваемых данных, содержащих информацию пользователей и/или системы управления СЭС.

Под *устойчивостью функционирования сети электросвязи* подразумевается способность сети электросвязи выполнять свои функции при выходе из строя части элементов сети в результате дестабилизирующих воздействий.

Меры обеспечения безопасности включают в себя набор функций, определяющих возможности механизмов обеспечения безопасности СЭС по непосредственной или косвенной реализации требований к безопасности. *Механизмом обеспечения безопасности сети электросвязи* является взаимоувязанная совокупность организационных, аппаратных, программных и программно-аппаратных средств, способов, методов, правил и процедур, используемых для реализации требований к безопасности СЭС.

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

Под *риском нарушения безопасности сети электросвязи* понимается вероятность причинения ущерба СЭС или ее компонентам вследствие того, что определенная угроза реализуется в результате наличия определенной уязвимости в СЭС. *Угрозой безопасности сети электросвязи* является совокупность условий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба СЭС или ее компонентам. *Уязвимость сети электросвязи* определяется как недостаток или слабое место в средстве связи, техническом процессе

(протоколе) обработки/передачи информации, мероприятиях и механизмах обеспечения безопасности СЭС, позволяющие нарушителю совершать действие, приводящее к успешной реализации угрозы безопасности.

Система обеспечения безопасности системы связи общего пользования (ССОП) - это совокупность служб безопасности операторов СЭС ССОП и используемых ими механизмов обеспечения безопасности, взаимодействующая с органами управления СЭС, организация и функционирование которой осуществляется по нормам, правилам и обязательным требованиям, установленным в области связи. Под *службой безопасности сети электросвязи* понимается организационно-техническая структура оператора СЭС, реализующая политику безопасности оператора связи и обеспечивающая функционирование системы обеспечения безопасности ССОП. *Политикой безопасности оператора связи* является совокупность документированных правил, процедур, практических приемов или руководящих принципов в области обеспечения безопасности, которыми должен руководствоваться оператор связи.

Сеть связи — технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи. Под *электросвязью* понимаются любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической или другим электромагнитными системами.

Контрольные вопросы и задания

1. Что понимается под безопасностью сети электросвязи?
2. Приведите пример дестабилизирующего воздействия на сеть электросвязи.
3. В чем разница между понятиями «безопасность сети электросвязи» и «устойчивость функционирования сети электросвязи»?
4. Определите соотношение между понятиями «меры обеспечения безопасности» «механизмы обеспечения безопасности».
5. Отличается ли понимание термина «риск нарушения безопасности сети электросвязи» от понимания термина «риск», выраженного в ГОСТ Р 51898 «Аспекты безопасности. Правила включения в стандарты»?
6. Проведите сопоставительный анализ определений терминов «угроза безопасности сети электросвязи» и «угроза» (в трактовке ГОСТ Р ИСО/МЭК 13335-1), а также «уязвимость сети электросвязи» и «уязвимость» (также в трактовке ГОСТ Р ИСО/МЭК 13335-1) на предмет выявления существенных различий.

1.2 Модель безопасности сети электросвязи

Взаимосвязь основных понятий и процессов обеспечения безопасности СЭС показана на рисунке 1.

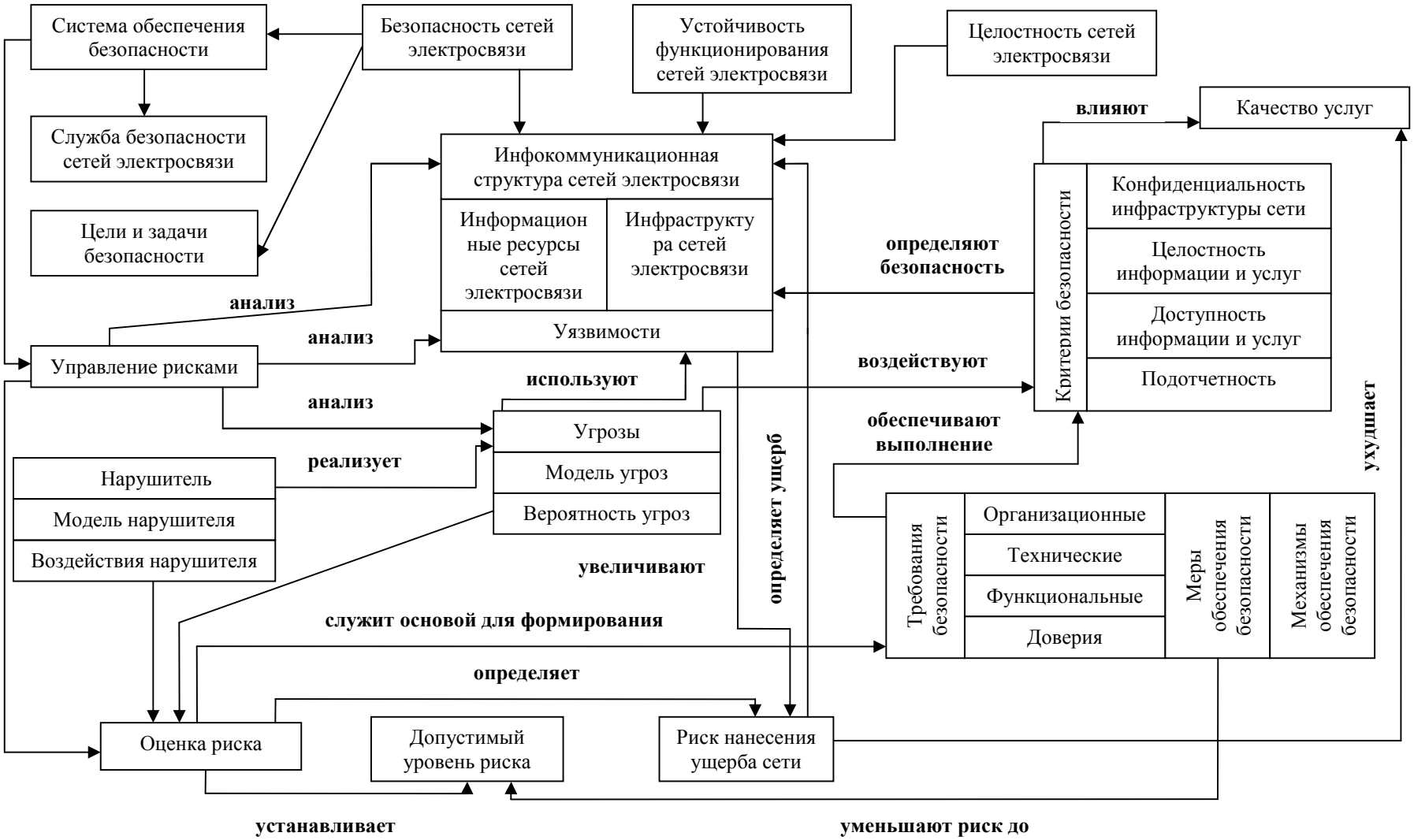

Рисунок 1 - Модель безопасности сети электросвязи

Контрольные вопросы

1. Приведите пример уязвимости какого-либо информационного ресурса.
2. Верно ли с точки зрения логики причинно-следственных связей утверждение о том, что требования безопасности обеспечивают выполнение критериев безопасности?
3. Корректно ли говорить о нанесении ущерба сети? Может ли сеть «ощущать» себя ущербной или ущерб причиняется собственнику сети?

1.3 Основные положения по обеспечению безопасности сетей электросвязи

1.3.1 Сети электросвязи, их информационные ресурсы, проблемы обеспечения безопасности сетей электросвязи

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 сетей электросвязи является не определяющим), и служебную информацию (например, адрес получателя). Сеть электросвязи должна обеспечить целостность передаваемых сообщений и своевременность их доставки адресату. Открытость СЭС не должна означать полную доступность ко всем ее информационным ресурсам и отсутствие контроля их использования. В СЭС должна быть обеспечена защита собственной, служебной информации, предназначенной для управления работой сети или служб сети.

К информационным ресурсам СЭС, требующим защиту со стороны оператора связи, могут быть отнесены:

– сведения об абонентах, базах данных;

– информация управления;

– данные, содержащие информацию пользователей (обеспечение доступности и целостности);

– программное обеспечение систем управления СЭС;

– 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 СЭС.

Необходимость рассмотрения проблемы обеспечения безопасности СЭС обусловлена:

– динамикой развития сетей электросвязи и их интеграцией с глобальными сетями связи, в том числе с Интернет;

– совершенствованием применяемых информационных технологий;

– 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 СЭС необходимых механизмов обеспечения безопасности.

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

– организации эффективного безопасного управления и взаимодействия сетей;

– поддержания гарантированных качественных характеристик процессов обработки информации в СЭС (качества обслуживания) в условиях возможных воздействий нарушителя на инфокоммуникационную структуру СЭС;

– создания в СЭС 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 СЭС, в том числе экстремистским действиям.

Решение данных проблем является функцией системы обеспечения безопасности сетей электросвязи ССОП и служб безопасности операторов связи в рамках общих положений по безопасности СЭС.

1.3.2 Основные цели и задачи обеспечения безопасности сетей электросвязи, обязанности оператора связи

Основными целями обеспечения безопасности СЭС являются:

– достижение устойчивого функционирования и успешного выполнения заданных функций СЭС, в условиях возможного воздействия

нарушителя, способного привести к нарушению конфиденциальности, целостности, доступности или подотчетности;

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

Основными задачами обеспечения безопасности СЭС являются:

– своевременное выявление, оценка и прогнозирование источников угроз безопасности, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития СЭС на всех уровнях иерархии единой сети электросвязи России (в международном, междугороднем, зоновом, местном, на уровне пользования услугами связи и т. д.);

– выявление и устранение уязвимостей в средствах связи и СЭС;

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

– организация системы пропуска приоритетного трафика по СЭС в случае чрезвычайных ситуаций, организация бесперебойной работы международной аварийной службы;

– совершенствование и стандартизация применяемых мер обеспечения безопасности СЭС.

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

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

На каждой стадии жизненного цикла СЭС (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 СЭС должна производиться на основе анализа уязвимостей СЭС и угроз, способных реализовать эти уязвимости.

1.3.3 Угрозы безопасности сети электросвязи, модель угроз безопасности сети электросвязи

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

За основу классификации угроз безопасности СЭС рекомендуется брать классификацию, установленную национальным стандартом 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.

Источниками угроз безопасности СЭС могут быть: субъект, материальный объект или физическое явление.

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

Полное множество угроз безопасности не поддается формализации. Это связано с тем, что архитектура современных СЭС, 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 СЭС.

К основным возможным угрозам безопасности СЭС могут быть отнесены следующие угрозы:

– уничтожение информации и/или других ресурсов;

– искажение или модификация информации;

– мошенничество;

– кража, утечка, потери 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 для нарушителя побуждение, чтобы реализовать угрозу
Возможно	На СЭС отсутствуют механизмы обеспечения безопасности, используемые для противодействия этой угрозе, и побуждение для нарушителя весьма высоко

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

Модель угроз безопасности СЭС 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) СЭС, требующих защиты;

– описание источников формирования дестабилизирующих воздействий и их потенциальных возможностей;

– стадии жизненного цикла СЭС, 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 СЭС с описанием обстоятельств, связанных с обнаружением нарушений.

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

1.3.4 Нарушители безопасности сети электросвязи, модель нарушителя

Угрозы безопасности СЭС 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 СЭС или конкретного протокола, если она своевременно не устраняется разработчиком или по его представлению службами эксплуатации оператора связи.

Нарушителями безопасности СЭС 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 организации связи;

– недобросовестные сотрудники и партнеры;

– пользователи услугами связи и др.

Основными мотивами нарушений безопасности СЭС могут быть:

– месть;

– достижение денежной выгоды, в том числе за счет продажи полученной информации;

– хулиганство и любопытство;

– профессиональное самоутверждение.

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

Задача построения модели нарушителя безопасности СЭС 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.

1.3.5 Направленность и характер воздействий нарушителя безопасности сети электросвязи

Воздействия нарушителя, в основном, направлены на ухудшение качественных характеристик СЭС и могут осуществляться, как правило, путем поиска и использования эксплуатационных и технологических уязвимостей. Воздействия нарушителя 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.

Воздействия нарушителя могут носить как непреднамеренный (случайный) характер, 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.

Активные действия нарушителя предусматривают вмешательство в работу СЭС, 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.

Пассивные действия нарушителя предполагают нанесение вреда абоненту (пользователю услугами связи) путем использования выявленных уязвимостей СЭС, 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.

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

1.3.6 Критерии безопасности сети электросвязи, последствия нарушений безопасности сети электросвязи

Безопасность СЭС характеризуется основными ее критериями:

– конфиденциальностью инфокоммуникационной структуры СЭС;

– целостностью информации и услуг связи;

– доступностью информации и услуг связи;

– подотчетностью действий в сети.

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

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

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

Нарушение целостности – несанкционированная модификация или разрушение информационных ресурсов и инфраструктуры СЭС.

Под доступностью информации и услуг понимается способность СЭС обеспечить пользователям согласованные условия доступа к предоставляемым услугам связи и их получение, в том числе в условиях

возможных воздействий нарушителя на инфокоммуникационную структуру СЭС.

Нарушение доступности – нарушение доступа к использованию информации и услуг связи.

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

Нарушение подотчетности – это 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	+	+	+	-
Несанкционированный доступ	+	+	+	+
Отказ в обслуживании	-	-	+	-

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

– «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

1.3.7 Принципы обеспечения безопасности сети электросвязи в условиях воздействия нарушителя

Обеспечение безопасности СЭС в условиях воздействия нарушителя должно осуществляться с учетом следующих основных принципов:

1) Комплексности использования всей совокупности нормативных правовых актов, организационных и режимных мер, программных, аппаратных и программно-аппаратных методов защиты, обеспечивающих безопасное функционирование СЭС.

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 СЭС, обеспечения соблюдения операторами связи предъявляемых им требований к безопасности, добросовестной конкуренции и защиты персональных данных пользователей.

3) Управляемости методами, действиями и процедурами по обеспечению безопасности СЭС и контролю качества процессов передачи информации в условиях возможных воздействий нарушителя на инфокоммуникационную структуру сетей в соответствии с функциями системы управления сетью.

4) Непрерывности совершенствования методов, действий и процедур по обеспечению безопасности СЭС с учетом достигнутого отечественного и зарубежного опыта в условиях возможных воздействий нарушителя и изменения методов и средств этих воздействий.

5) Совместимости аппаратно-программных средств и технологий, применяемых в системах обеспечения безопасности.

Контрольные вопросы и задания

1. Является ли открытой сеть электросвязи, в которой отсутствуют полная доступность ко всем ее информационным ресурсам и имеется контроль их использования.
2. Устойчивость функционирования сети электросвязи обеспечивает ее безопасность или наоборот?
3. Какими факторами может устанавливаться при идентификации предел количества угроз безопасности сети электросвязи?
4. Является ли несанкционированный доступ сам по себе угрозой или же методом осуществления угрозы?
5. Разработайте модель угроз безопасности для корпоративной сети телефонной связи вуза.
6. Разработайте модель нарушителя безопасности для корпоративной сети телефонной связи вуза.
7. Верно ли и почему утверждение, что «воздействия нарушителя, в основном, направлены на ухудшение качественных характеристик сети электросвязи»?
8. Конфиденциальность инфокоммуникационной структуры сети электросвязи, целостность информации и услуг связи, доступность

информации и услуг связи, подотчетность действий в сети – это критерии или характеристики безопасности сети электросвязи?

9. От чего больше зависит безопасность сети электросвязи в условиях воздействия нарушителя: от совместимости аппаратно-программных средств и технологий, применяемых в системах обеспечения безопасности, или от совместимости основных функциональных аппаратно-программных средств и технологий электросвязи?

1.4 Общие требования к безопасности сетей электросвязи

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

Требования к безопасности СЭС 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 СЭС должны формулироваться с учетом:

– целей, функций и задач, решаемых оператором связи;

– условий использования СЭС в общей системе связи государства;

– специфики используемой технологии передачи информации;

– потенциальных угроз безопасности и возможных воздействий нарушителя;

– реальных проектных и эксплуатационных ресурсов и существующих ограничений на функционирование СЭС;

– требований и условий взаимодействия с другими СЭС.

Предоставление и использование услуг и механизмов обеспечения безопасности может быть довольно дорогим относительно потерь при нарушении безопасности СЭС. 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 СЭС включают:

– организационные требования безопасности (ОТБ);
– технические требования безопасности (ТТБ);
– функциональные требования безопасности (ФТБ);
– требования доверия к безопасности (ТДБ).

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 СЭС.

ФТБ и ТДБ содержат требования, которые для сетей и средств связи излагаются в профилях защиты и заданиях по безопасности и должны реализовываться на всех этапах жизненного цикла СЭС[1].

Контрольные вопросы

1. Чем отличаются административные положения и процедуры по осуществлению мероприятий политики безопасности оператором связи от организационных?
2. Требования к безопасности сетей электросвязи устанавливают федеральные органы исполнительной власти в области связи или федеральные органы исполнительной власти в области безопасности, технической защиты информации и противодействия техническим разведкам?
3. Что является основным критерием масштаба системы мер обеспечения безопасности сетей электросвязи?

1.5 Основные мероприятия по обеспечению безопасности сетей электросвязи

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

[1] Следует отметить, что требования ГОСТ Р ИСО/МЭК 15408 практически мало подходят для систем информационных технологий, а тем более для таких распределенных и сложных систем как сети электросвязи.

Мероприятия по обеспечению безопасности СЭС, 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 СЭС с привлечением по необходимости специализированных организаций, имеющих лицензию 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 СЭС к другой и условия выполнения обязательных требований к безопасности, установленных федеральными органами исполнительной власти в области связи, при взаимодействии этих сетей оговариваются в заключаемых операторами связи договорах о присоединении СЭС.

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

Обеспечение безопасности СЭС достигается:

а) защитой СЭС от несанкционированного доступа 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 несанкционированных воздействий, включая физическую защиту сооружений и линий связи;

д) разграничением доступа пользователей и субъектов инфокоммуникационной структуры СЭС 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 СЭС;

з) использованием организационных методов, включающих:

1) разработку и реализацию политики безопасности оператором связи;

2) организацию контроля состояния безопасности СЭС;

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

4) определение порядка реагирования на инциденты безопасности;

5) разработку программ повышения информированности персонала СЭС в вопросах понимания ими проблем безопасности;

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

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

Взаимоотношения пользователей с операторами связи в сфере обеспечения безопасности СЭС должны строиться на основании следующих положений:

– только авторизованные пользователи должны иметь доступ к СЭС 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 СЭС.

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.

Контрольные вопросы и задания

1. Является ли противодействие сетевым атакам и вирусам механизмом обеспечения безопасности?
2. Приведите известные примеры предоставления оператором связи пользователям услугами связи дополнительных услуг по защите информации и процесса безопасной передачи сообщений на договорной основе.
3. Разработайте план возможной реализации оператором телефонной связи обязанности по информированию пользователей о состоянии безопасности доступа к услугам телефонной связи.
4. Допустимо ли отключение механизмов обеспечения безопасности сетей электросвязи, если мероприятия по обеспечению безопасности СЭС, проводимые оператором связи, ухудшают качественные характеристики сети и снижают оперативность обработки информации?

1.6 Основные положения о структуре системы обеспечения безопасности сетей электросвязи

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

Архитектура СОБ СЭС 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.

Архитектура СОБ СЭС 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 СЭС, координируемое центральным органом СОБ;

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

1) взаимодействие с системой управления СЭС;

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

3) учет практического применения нормативной правовой базы (законов, 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 СЭС;

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 воздействий нарушителя 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) передачу 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.

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

Деятельность органов СОБ СЭС подразумевает выполнение следующих мероприятий:

– подтверждение соответствия средств связи, паспортизацию организаций связи и аттестацию объектов и СЭС по требованиям безопасности;

– оценку состояния безопасности СЭС, прогнозирование и обнаружение внутренних и внешних угроз безопасности;

– анализ информационных рисков, создание систем управления рисками и страхования информационных рисков;

– выявление уязвимостей в СЭС и осуществление комплекса адекватных и экономически обоснованных мер по их снижению;

– предотвращение, либо обнаружение воздействия нарушителя, пресечение их реализации, локализацию и ликвидацию последствий этих дестабилизирующих воздействий на инфокоммуникационную структуру СЭС;

– оповещение о нарушении безопасности, реакцию на инциденты безопасности и восстановление нарушенного процесса функционирования СЭС;

– адаптацию СОБ к изменяющимся условиям функционирования СЭС;

– контроль качества обслуживания в условиях воздействия нарушителя;

– 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 СЭС с учетом рекомендаций и стандартов международных организаций по стандартизации;

– реализацию мер по обеспечению безопасности СЭС, основой которых является применение соответствующих механизмов обеспечения безопасности.

Контрольные вопросы

1. Перечислите уровни безопасности в архитектуре системы обеспечения безопасности.
2. Чем уровень безопасности инфокоммуникационной структуры отличается от уровня сетевой безопасности?
3. Идентичны ли понятия «информационный риск» и «риск нарушения безопасности сети электросвязи»? Что такое информационный риск

2 Общие критерии оценки безопасности информационных технологий

2.1 Основные понятия и идеи Общих Критериев

Общие Критерии содержат два основных вида требований безопасности:

– функциональные требования, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;

– требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности формулируются и их выполнение проверяется для определенного объекта оценки (ОО) аппаратно-программного продукта ИТ или системы ИТ.

Безопасность в ОК рассматривается на жизненном цикле ОО. Кроме того, ОО рассматривается в контексте среды безопасности,

характеризующейся определенными условиями и угрозами. Требования в ОК формулируются в виде документов двух видов:

– профиля защиты (ПЗ);

– задания по безопасности (ЗБ).

Профиль защиты - это типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса.

Задания по безопасности содержат совокупность требований к конкретной разработке продукта или системы.

Системой ИТ называется специфичная реализация ИТ с конкретным назначением и условиями эксплуатации.

Продукт ИТ же представляет собой совокупность средств ИТ, предоставляющих определенные функциональные возможности и предназначенных для непосредственного использования либо включения в различные системы.

Продукт или система могут быть уже существующими либо проектируемыми.

В среду безопасности ОО включаются:

– законодательная среда (нормативные акты, затрагивающие ОО);

– административная среда (положения политик и программ безопасности, учитывающих особенности ОО);

– процедурная среда (физическая среда ОО и меры его физической защиты, персонал и его свойства, принятые эксплуатационные и иные процедуры);

– программно-техническая среда (предназначение ОО и предполагаемые области его применения, активы (ресурсы), которые требуют защиты средствами ОО).

Из анализа среды безопасности должны быть описаны следующие аспекты:

1) предположение безопасности, которое выделяет ОО из общего контекста, задает границы рассмотрения. Истинность этих предположений принимается бездоказательно, а из множества возможных отбираются только те, что заведомо необходимы для обеспечения безопасности ОО;

2) угрозы безопасности ОО, наличие которых в рассматриваемой среде установлено или предполагается. Они характеризуются несколькими параметрами:

– источник;

– метод воздействия;

– опасные с точки зрения закономерности использования уязвимости;

– активы, потенциально подверженные повреждению.

При анализе рисков реализации угроз принимается во внимание вероятность активизации угрозы и ее успешного осуществления, а также размер возможного ущерба. По результатам анализа из множества допустимых угроз отбираются только те, ущерб от которых нуждается в уменьшении;

3) положения политики безопасности, предназначенные для применения к ОО. Для системы ИТ такие положения могут быть описаны точно, для продукта ИТ — в общих чертах.

На основании предположений, при учете угроз и положений политики безопасности формулируются цели безопасности для объекта оценки, направленные на обеспечение противостояния угрозам и выполнение политики безопасности. В зависимости от непосредственного отношения к объекту оценки или среде они делятся на цели безопасности ОО и цели безопасности среды. На основании сформулированных целей безопасности выбираются требования безопасности

ОК, а именно их вторая и третья части, являются каталогами требований безопасности.

В основу методологии ОК положена модель безопасности, представленная на рисунке 2.

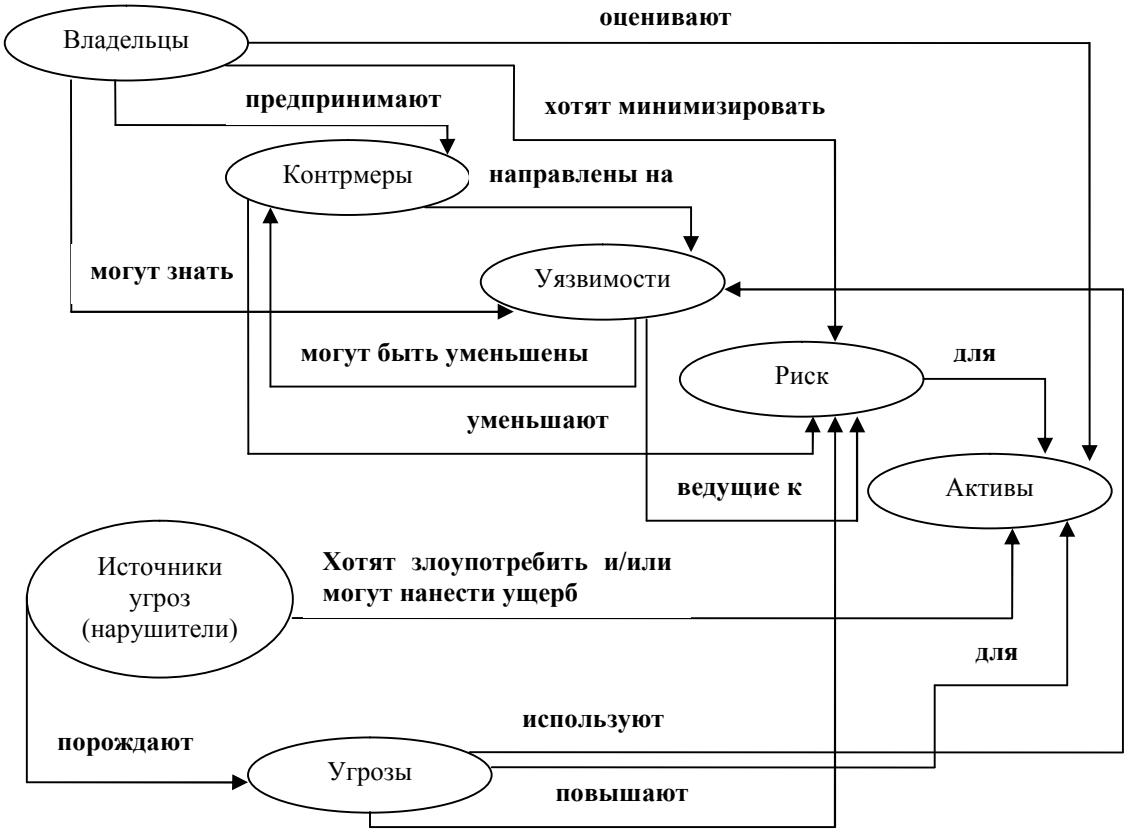

Рисунок 2 - Модель безопасности, положенная в основу методологии ОК

Для структуризации пространственных требований в ОК введена иерархия класс – семейство – компонент - элемент.

Классы определяют наиболее общую группировку требований.

Семейства в пределах класса различаются по строгости и другим характеристикам требований.

Компонент определяется минимальным набором требований, фигурирующим как единое целое.

Элемент — это неделимое требование безопасности.

Между критериями введены зависимости, возникающие, когда компонент сам по себе недостаточен для достижения целей безопасности.

После формулирования функциональных требований и требований доверия к ОО и его среде в ПЗ и в ЗБ можно приступать к оценке безопасности продукта или системы.

ПЗ по своему составу отличается от ЗБ двумя разделами. В ЗБ добавляется краткая спецификация ОО и утверждение о соответствии профилю защиты.

ПЗ включает в себя следующие разделы:

– введение, состоящее из разделов идентификации ПЗ и аннотации ПЗ;

– описание ОО;

– среда безопасности ОО, состоящая из подразделов предположений безопасности, угрозы, политики безопасности организации;

– цели безопасности, состоящие из подразделов целей безопасности для ОО и целей безопасности для среды;

– требования безопасности ИТ, состоящие из требований безопасности для ОО, включая функциональные требования безопасности ОО, требований доверия безопасности к ОО и требований безопасности для среды ИТ;

– замечания по применению и обоснование, состоящее из подразделов логического обоснования требований безопасности и логического обоснования целей безопасности.

Состав ЗБ отличается наличием двух разделов и нескольких подразделов. Дополнительно в ЗБ имеются следующие разделы:

– краткая спецификация ОО, состоящая из функций безопасности ОО и спецификации мер доверия;

– утверждение соответствия ПЗ, в котором приводится ссылка на ПЗ, конкретизация ПЗ и дополнение ПЗ.

Раздел введение дополняется разделом соответствия ОК. В раздел обоснование добавляются раздел логического обоснования краткой спецификации ОО и логического обоснования утверждения о соответствии ПЗ.

Краткая спецификация определяет отображение требований на функции безопасности.

ОК не предписывают конкретные методологии или дисциплины разработки продуктов и систем ИТ, но предусматривают наличие нескольких уровней представления проекта с его декомпозицией и детализацией.

За требованиями безопасности следует функциональная спецификация, затем проект верхнего уровня, необходимое число промежуточных уровней, проект нижнего уровня, исходный код или схема аппаратуры и реализация в виде исполняемых файлов, аппаратных продуктов и т.п. Между уровнями представления должно демонстрироваться соответствие, то есть все сущности более высоких уровней обязаны фигурировать и ниже, а внизу не должно быть места

лишним сущностям, необусловленным потребностями более высоких уровней.

При проведении оценки главными являются следующие вопросы:

1) отвечают ли функции безопасности ОО функциональным требованиям?

2) конкретна ли реализация функций безопасности?

Если оба ответа положительны, то говорят о достижении целей безопасности.

Контрольные вопросы

1. Опишите алгоритм формирования требований безопасности, используемый в Общих критериях.

2. Можно ли при создании безопасных систем информационных технологий в соответствии с подходами Общих критериев использовать алгоритм создания автоматизированной системы, предписываемый ГОСТ 34.601 «Автоматизированные системы. Стадии создания»?

3. Каков состав задания по безопасности и чем он отличается от состава профиля защиты?

4. Какими параметрами характеризуется в Общих критериях угроза безопасности объекта оценки?

5. Из каких сущностей (класс, семейство, компонент или элемент) формируются профиль защиты и задание по безопасности?

6. Почему для системы ИТ положения политики безопасности могут быть описаны при ее создании точно, а для продукта ИТ — только в общих чертах?

2.2 Классификация функциональных требований безопасности

Часть вторая ОК описывает 11 классов, 66 семейств, 135 компонентов функциональных требований безопасности и содержит сведения о том, какие цели безопасности могут быть достигнуты при современном уровне ИТ и каким образом. Функциональные компоненты могут быть не до конца конкретизированы в ОК, поэтому фактические параметры подставляются в ПЗ и ЗБ. Такая операция называется назначением. В качестве параметров могут выступать, например, такие сложные сущности, как политика безопасности.

Некоторые компоненты в ОК задаются с «запросом». В них включается список возможностей, из которых потом осуществляется выбор той, что необходима в конкретной ситуации, например,

обнаружение и/или предотвращение определенных нарушений политики безопасности.

Любой функциональный компонент допускает операции по многократному использованию, например, для охвата различных аспектов ОО, называемые в ОК итерациями, а также уточнение и добавление дополнительных деталей.

Между компонентами функциональных требований могут существовать зависимости. Они возникают, когда компонент не является самодостаточным и для своей реализации нуждается в привлечении других компонентов.

Классы функциональных требований можно условно разделить в зависимости от того описывают ли они элементарные сервисы безопасности или производные, реализуемые на основе элементарных, направлены ли они на достижение высокоуровневых целей безопасности или играют инфраструктурную роль.

К первой группе можно отнести следующие классы:

– FAU - аудит безопасности;
– FIA - идентификация и аутентификация;
– FRU - использование ресурсов.

Класс FAU состоит из 6 семейств, содержащих требования к отбору, регистрации, хранению и анализу данных о действиях и событиях, затрагивающих безопасность объекта оценки. Класс FIA состоит из 6 семейств, содержащих требования к идентификации пользователя, к аутентификации пользователей, определению атрибутов пользователя, к связыванию пользователя с субъектом, к отказам аутентификации и к спецификации секретов. Класс FRU включает 3 семейства, призванные разными способами поддерживать высокую доступность: отказоустойчивость, приоритет обслуживания и распределение ресурсов.

Ко второй группе можно отнести следующие классы:

– FCO – связь;
– FPR — приватность.

Класс FCO состоит из 2 семейств, обеспечивающих неотказуемость отправки или получения данных, которая достигается путем избирательной или принудительной генерации, допускающих верификацию свидетельств, позволяющих ассоциировать атрибуты отправителя (получателя) с элементами передаваемых данных. Класс FPR содержит 4 семейства, обеспечивающих защиту пользователя от раскрытия и несанкционированного использования его идентификационных данных: анонимность, псевдонимность, невозможность ассоциаций и скрытность.

Достичь высокоуровневых целей безопасности помогают два класса:

– FDP — защита данных пользователя;

– FPT — защита функций безопасности ОО.

Класс FDP включает 13 семейств, которые можно разбить на четыре группы:

– политики защиты данных пользователя;

– виды защиты данных пользователя;

– импорт и экспорт данных пользователя;

– защита данных пользователя при передаче между доверенными продуктами и системами информационных технологий.

Класс FPT включает 16 семейств, которые можно условно разделить на четыре группы:

– архитектурная безопасность;

– защита реализаций функций безопасности;

– защита данных функций безопасности;

– инфраструктурные требования.

Наибольшее число компонентов сосредоточено в классах инфраструктурной группы:

– FCS — криптографическая поддержка;

– FMT — управление безопасностью;

– FTA — доступ к ОО;

– FTP — доверенный маршрут/канал.

Класс FCS состоит из двух семейств, где в самом общем виде (в виде параметризованных шаблонов) рассматриваются генерация, распределение, доступ и уничтожение ключей, а также криптографические операции. Смысл требований состоит в том, что необходимо действовать в соответствии с некими алгоритмами, длинами ключей и стандартами. Какие-либо содержательные специфики отсутствуют. Класс FMT, включающий шесть семейств, регламентирует управление функциями безопасности и их данными, атрибутами и ролями безопасности. Класс FTA содержит шесть семейств, куда вошли требования управления сеансами работы пользователей (помимо идентификации и аутентификации). Класс FTP, состоящий из двух семейств: «доверенный маршрут» и «доверенный канал» – обеспечивает требования по созданию маршрутов/каналов передачи информации безопасным образом.

Контрольные вопросы

1. На базе каких элементарных сервисов безопасности первой группы классов функциональных требований могут быть реализованы требования второй группы функциональных требований класса FCO?
2. Чем отличается доверенный маршрут от доверенного канала?
3. Почему требования класса FTA отнесены условно к инфраструктурной группе?
4. Обеспечивает ли реализация требований класса FPR абсолютную неподотчетность действий пользователя в системе?

2.3 Пример описания функциональных требований

Рассмотрим описание класса, семейства, компонента и элементов требований на примере класса FCO «Связь».

Класс FCO содержит два семейства, связанные с уверенностью в идентичности сторон, участвующих в обмене данными: идентичностью отправителя переданной информации (доказательство отправления) и идентичностью получателя переданной информации (доказательство получения). Эти семейства обеспечивают, что отправитель не сможет отрицать факт отправления сообщения, а получатель не сможет отрицать факт его получения.

Декомпозиция класса на составляющие его компоненты показана на рисунке 3

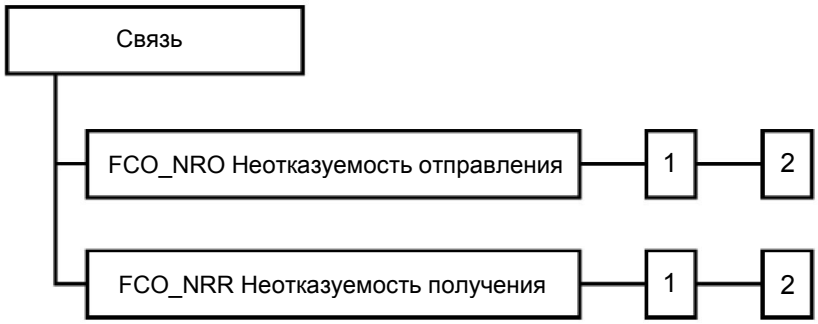

Рисунок 3 – Декомпозиция класса FCO «Связь»

Семейство FCO_NRO «Неотказуемость отправления» обеспечивает невозможность отрицания отправителем информации факта ее отправления. Семейство FCO_NRO содержит требование, чтобы функции безопасности объекта оценки обеспечили метод предоставления субъекту-получателю свидетельства отправления информации. Это свидетельство может быть затем верифицировано этим субъектом или другими субъектами.

Ранжирование компонентов показано на рисунке 4

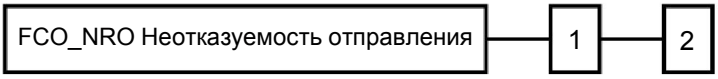

Рисунок 4 - Ранжирование компонентов семейства FCO_NRO

FCO_NRO.1 «Избирательное доказательство отправления» содержит требование, чтобы функции безопасности объекта оценки предоставили субъектам возможность запросить свидетельство отправления информации.

FCO_NRO.2 «Принудительное доказательство отправления» содержит требование, чтобы функции безопасности объекта оценки всегда генерировали свидетельство отправления передаваемой информации.

Управление: FCO_NRO.1, FCO_NRO.2

Для функций управления из класса FMT может рассматриваться следующее действие.

а) Управление изменениями типов и полей информации, атрибутов отправителей информации и получателей свидетельств.

Аудит: FCO_NRO.1

Если в профиль защиты или задание по безопасности включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность (в зависимости от выбранного уровня) аудита следующих действий/событий/параметров.

а) Минимальный: идентификатор пользователя, который запросил генерацию свидетельства отправления.

б) Минимальный: обращение к функции неотказуемости.

в) Базовый: идентификатор информации, получателя и копии предоставляемого свидетельства.

г) Детализированный: идентификатор пользователя, который запросил верификацию свидетельства.

Аудит: FCO_NRO.2

Если в профиль защиты или задание по безопасности включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность (в зависимости от выбранного уровня) аудита следующих действий/событий/параметров.

а) Минимальный: обращение к функции неотказуемости.

б) Базовый: идентификация информации, получателя и копии предоставляемого свидетельства.

в) Детализированный: идентификатор пользователя, который запросил верификацию свидетельства.

Описание компонента FCO_NRO.1 «Избирательное доказательство отправления» выглядит следующим образом.

Иерархический для FCO_NRO.1: нет подчиненных компонентов.

Элементы компонента FCO_NRO.1 описаны ниже.

FCO_NRO.1.1 ФБО должны быть способны генерировать свидетельство отправления передаваемой [назначение: *список типов информации*] при запросе [выбор: *отправитель, получатель, [назначение: список третьих лиц]*].

FCO_NRO.1.2 ФБО должны быть способны связать [назначение: *список атрибутов*] отправителя информации и [назначение: *список информационных полей*] информации, к которой прилагается свидетельство.

FCO_NRO.1.3 ФБО должны предоставить возможность верифицировать свидетельство отправления информации [выбор: *отправитель, получатель, [назначение: список третьих лиц]*] при установленных [назначение: *ограничения на свидетельство отправления*]

Зависимости: FIA_UID.1 Выбор момента идентификации

Выбор и назначение – здесь операции которые возможно проводить над элементами требований при их описании в профиле защиты или задании по безопасности для типов или конкретных объектов оценки.

Контрольные вопросы

1. Почему без компонента FIA_UID.1 «Выбор момента идентификации» компонент FCO_NRO.1 является несамодостаточным и не может обеспечить выполнение соответствующих целей безопасности?

2. Объясните полный алгоритм взаимоотношений между компонентом FCO_NRO.1 и соответствующими компонентами из класса FMT в части управления изменениями типов и полей информации, атрибутов отправителей информации и получателей свидетельств.

3. С какой целью может быть потребован в профиле защиты или задании по безопасности детализированный уровень аудита с регистрацией идентификатора пользователя, который запросил верификацию свидетельства?

2.4 Основные понятия и классификация требований доверия безопасности

Доверие в интерпретации ОК — это основа для уверенности в том, что продукт или система ИТ отвечают целям безопасности. Доверие обеспечивается через активные исследования (оценку) продукта или системы.

Требования доверия безопасности охватывают весь жизненный цикл ОО и предполагают выполнение следующих действий:

– оцениваются ЗБ и ПЗ, как источники требований безопасности;

– анализируются различные представления проекта ОО и соответствие между ними, а также соответствие каждого из них требованиям безопасности;

– проверяются процессы и процедуры безопасности, их применение, анализируется документация, верифицируются представленные доказательства;

– анализируются тесты и их результаты, а также уязвимости ОО;

– проводится независимое тестирование, в том числе тестирование проникновением.

Каждое требование (элемент) доверия принадлежит одному из трех типов:

– элементы действия разработчика (помечаются буквой D после номера элемента). Эти действия должны подтверждаться доказательным материалом (свидетельством);

– элементы представления и содержания свидетельств (помечаются буквой S);

– элементы действия оценщика (помечаются буквой E).

Оценщики обязаны проверить представленные разработчиками свидетельства, а также выполнить необходимые дополнительные действия, например, провести независимое тестирование.

Требования доверия разделены на 10 классов, 44 семейства, 93 компонента. Классы можно сгруппировать в зависимости от охватываемых этапов жизненного цикла ОО.

К первой группе, логически предшествующей разработке и оценке ОО, принадлежат классы:

– APE — оценка ПЗ;

– ASE — оценка ЗБ.

Цель требований классов APE и ASE - проверить полноту, непротиворечивость и реализуемость профиля защиты или задания по безопасности.

Во вторую группу входят классы:

– ADV — разработка;

– ALC — поддержка жизненного цикла;

– ACM — управление конфигурацией.

Класс ADV (разработка) состоит из семи семейств и содержит требования для постепенного повышения уровня детализации проекта вплоть до представления реализаций с демонстрацией соответствия между уровнями. В этом классе предусмотрено три стиля изложения спецификации: неформальный, полуформальный и формальный – и три способа демонстрации соответствия. Технологические требования процедурного характера составляют содержание класса ALC (поддержка жизненного цикла), состоящего из четырех семейств. Прежде всего, определяется модель жизненного цикла (семейство ALC_LCD), затем следует обосновать выбор инструментальных средств и методов (семейство ALC_TAD). Безопасность разработки организуется в соответствии с требованиями семейства ALC_DVC. Важнейшим элементом этапа сопровождения является устранение недостатков (семейство ALC_FLR). Управление конфигурацией (класс ACM) - необходимый инструмент коллектива разработчиков. В этот класс входят три семейства, самое содержательное из которых ACM_CAB, специфицирующее возможности управления конфигурацией. Семейство ACM_SCP специфицирует область действия управления конфигурацией. Для уменьшения числа возможных ошибок управление конфигурацией следует максимально автоматизировать. В этом состоит смысл требований семейства ACM_AOT.

К этапу получения, представления и анализа результатов разработки можно отнести классы:

– AGD — руководство пользователя, администратора;

– ATE — тестирование;

– AVA — оценка уязвимостей.

Класс AGD состоит из двух семейств, где сформулированы требования к руководствам администратора (AGD_ADM) и пользователя (AGD_USR). Класс ATE состоит из четырех семейств, содержащих требования к полноте, глубине, способам и результатам тестирования функций безопасности на предмет их соответствия спецификациям. Один из ключевых моментов оценки безопасности продуктов информационных

технологий – это оценка уязвимостей (класс AVA), отправным пунктом которой является анализ уязвимостей (семейство AVA_VLA), выполняемый разработчиком и оценщиком. Анализ стойкости функций безопасности объекта оценки (семейство AVA_SOF) проводится на уровне реализующих механизмов. Требования семейства AVA_MSV (неправильное применение) направлено на то, чтобы исключить возможность такого конфигурирования и (или) применения объекта оценки, которое администратор или пользователь считает безопасным, в то время как оно таковым не является. Анализ скрытых каналов, регламентируемый семейством AVA_CCA, требует, чтобы разработчик проводил исчерпывающий поиск скрытых каналов для каждой политики управления информационными потоками и предоставлял документацию анализа, а оценщик должен выборочно подтвердить правильность анализа скрытых каналов посредством тестирования.

Класс ADO (поставка и эксплуатация) содержит требования к процедурам поставки, установки, генерации и запуска объекта оценки.

Класс AMA (поддержка доверия) включает требования, применяемые после сертификации ОО на соответствие ОК. Они помогают по возможности экономно, без полной повторной оценки, сохранять уверенность в том, что объект оценки продолжает отвечать своему заданию по безопасности после изменений в нем или его среде. Речь идет о выявлении новых угроз и уязвимостей, изменений в требованиях пользователей, об исправлении ошибок.

Компоненты требования доверия линейно упорядочены в пределах семейства, то есть компонент с большим номером всегда усиливает предыдущий.

Одна из целей ОК состоит в минимизации усилий оценщиков и разработчиков, направленных на обеспечение заданного уровня доверия. Этому способствует введение семи оценочных уровней доверия (ОУД), содержащих полезные для практического применения комбинации компонентов, упорядоченные по степени усиления. Повысить уровень доверия помогают дополнительные действия:

– расширение границ ОО;

– увеличение уровня детализации рассматриваемых аспектов ОО;

– повышение строгости рассмотрения и применения более формальных методов верификации.

Контрольные вопросы

1. Реализация требований доверия увеличивает защищенность объекта оценки или повышает уверенность в его защищенности у оценщика и потребителя?
2. Раскройте смысл понятия «скрытый канал» и поясните, могут ли они оставаться в действующем объекте оценки, если разработчик осуществлял их поиск в процессе разработки объекта оценки?
3. Позволяет ли применение требований класса AMA избежать переоценки действующего сертифицированного ранее объекта оценки?

2.5 Оценочные уровни доверия безопасности

В ОК определено 7 упорядоченных по возрастанию оценочных уровней доверия безопасности, содержащих рассчитанные на многократное применение комбинаций требования доверия (не более одного компонента из каждого семейства). Наличие такой шкалы дает возможность сбалансированного получения уровней доверия со сложностью, сроками, стоимостью и самой возможностью его достижения.

Предполагается, что в ПЗ и ЗБ будут фигурировать или сами ОУД, или их усиления, полученные путем расширения требований (за счет добавления к ОУД новых компонентов), либо увеличения строгости и (или) глубины оценки (посредством замены компонентов более сильным вариантом из того же семейства).

В ОУД не включены требования классов APE, ASE и AMA, поскольку они находятся за пределами основного цикла разработки продуктов и систем ИТ.

ОУД 1, предусматривающий функциональное тестирование, применим, когда требуется некоторая уверенность, что объект оценки работает безукоризненно, а угрозы безопасности не считаются серьезными. Его можно достичь без помощи разработчика и с минимальными затратами посредством анализа функциональной спецификации интерфейсов, эксплуатационной документации в сочетании с независимым тестированием.

ОУД 2, предусматривающий структурное тестирование и доступ к части проектной документации и результатам тестирования разработчиками, применим, когда разработчикам или пользователям требуется независимо получаемый умеренный уровень доверия при отсутствии доступа к полной документации по разработке. В дополнении к ОУД 1 предписывается анализ проекта верхнего уровня. Анализ должен быть поддержан независимым тестированием функции безопасности,

актом разработчика об испытаниях, основанных на функциональной спецификации, выборочном независимом подтверждении результатов тестирования разработчиком, анализом стойкости функций и свидетельством поиска явных уязвимостей. Требуется наличие списка конфигураций объекта оценки с уникальной идентификацией элементов конфигураций и свидетельства безопасных процедур поставки.

ОУД 3, предусматривающий систематическое тестирование и проверку, позволяет достичь максимально возможного доверия при использовании обычных методов разработки. Он применим в тех случаях, когда разработчикам или пользователям требуется умеренный уровень доверия на основе всестороннего исследования объекта оценки и процесса его разработки. По сравнению с ОУД 2 сюда добавлены требования, которые предписывают разработчику создавать акт об испытаниях с учетом особенностей не только функциональной спецификации, но и проекта верхнего уровня. Кроме того требуется контроль среды разработки и управление конфигурацией объекта оценки.

ОУД 4, предусматривающий систематическое проектирование, тестирование и просмотр, позволяет достичь доверия, максимально возможного при следовании общепринятой практике коммерческой разработки. Это самый высокий уровень, по которому, вероятно, экономически целесообразно ориентироваться для существующих типов продуктов. ОУД 4 характеризуется анализом функциональной спецификации, полной спецификацией интерфейсов, эксплуатационной документацией, проектом верхнего и нижнего уровней, а также подмножеством реализаций, применением неформальной модели политики безопасности объекта оценки. Среди других дополнительных требований выделяют независимый анализ уязвимостей, демонстрирующий устойчивость к попыткам проникновения нарушителей с низким потенциалом нападения, и автоматизацию управления конфигурацией.

Отличительная особенность ОУД 5 — это полуформальное проектирование и тестирование. С его помощью достигается доверие максимально возможное при следовании строгой практике коммерческой разработки, поддержанной умеренным применением специализированных методов обеспечения безопасности. ОУД 5 востребован, когда нужен высокий уровень доверия и строгий подход к разработке, не влекущий излишних затрат. Для достижения ОУД 5 требуется формальная модель политики безопасности объекта оценки, полуформальное представление функциональной спецификации и проект верхнего уровня, полуформальная демонстрация соответствия между ними, а также модульная структура объекта оценки. Акт об испытаниях должен быть

основан еще и на проекте нижнего уровня. Необходима устойчивость к попыткам проникновения нарушителей с умеренным потенциалом нападения. Предусматривается проверка правильности анализа разработчиком скрытых каналов и всестороннего управления конфигурацией.

ОУД 6, характеризующийся полуформальной верификацией проекта, позволяет получить высокое доверие путем применения специальных методов проектирования в строго контролируемой среде разработки при производстве высококачественных продуктов ИТ и при защите ценных активов от значительных рисков. Особенности ОУД 6:

– структурированное представление реализации;

– полуформальное представление проекта нижнего уровня;

– иерархическая структура проекта объекта оценки;

– устойчивость к попыткам проникновения нарушителей с высоким потенциалом нападения;

– проверка правильности систематического анализа разработчиком скрытых каналов;

– использование структурированного процесса разработки;

– полная автоматизация управления конфигурацией объекта оценки.

ОУД 7, предусматривающий формальную верификацию проекта, применим к разработке продуктов ИТ для использования в ситуациях чрезвычайно высокого риска или там, где высокая ценность активов оправдывает повышенные затраты. На седьмом уровне дополнительно требуется формальное представление функциональной спецификации, проекта верхнего уровня и формальная демонстрация соответствия между ними, модульная, иерархическая и простая структура проекта объекта оценки, добавление представления реализации, как основы акта об испытаниях, полное независимое подтверждение результатов тестирования разработчиком.

Контрольные вопросы

1. С какой целью в Общих критериях осуществлено группирование отдельных компонентов требований доверия в оценочные уровни доверия безопасности?

2. Можно ли изменять (если да, то каким образом) состав оценочных уровней доверия безопасности?

3. Какой максимальный оценочный уровень доверия может быть подтвержден при оценке объекта оценки без участия разработчика?

4. Объясните, что может считаться полуформальным представлением функциональной спецификации объекта оценки-программного продукта, используемым в ОУД 6?

5. Объясните различия между функциональным, структурным и систематическим тестированием объекта оценки, требуемым в ОУД 1 – ОУД 3.

6. Что такое систематическое проектирование, требуемое в ОУД 4?

3 Системы менеджмента информационной безопасности в организациях электросвязи

3.1 Процессный подход и модель систем менеджмента информационной безопасности телекоммуникаций

Для организаций электросвязи информация и вспомогательные процессы, устройства, сети и линии электросвязи являются важными активами бизнеса. Для должного управления этими активами бизнеса и для правильного и успешного продолжения бизнеса организаций электросвязи чрезвычайно важно управление информационной безопасностью.

Система менеджмента информационной безопасности (СМИБ) предназначается для обеспечения достаточных и соразмерных средств управления безопасностью, которые адекватно защищают информационные активы и придают уверенность клиентам и деловым партнерам организаций электросвязи, а также другим заинтересованным сторонам электросвязи. Это может служить средством поддержания и улучшения конкурентоспособности, увеличения денежных потоков и доходности, соблюдения правовых норм и улучшения коммерческой репутации.

СМИБ — это часть общей системы менеджмента, основанная на подходе бизнес-риска для установления, реализации, эксплуатации, мониторинга, анализа, обслуживания и усовершенствования информационной безопасности (ИБ).

Для эффективного функционирования организация электросвязи должна определять многие действия и управлять ими. Любое действие, использующее ресурсы и управляемое с целью создать возможность преобразования входных данных в выходные, может рассматриваться как процесс.

Часто выходные данные одного процесса непосредственно образуют входные данные следующего процесса.

Применение системы процессов внутри организации совместно с идентификацией и взаимодействием этих процессов, а также управлением ими может быть названо "подходом, основанным на процессах".

Подход, основанный на процессах, способствует акцентированию внимания его пользователей на важность:

– понимания требований бизнеса к информационной безопасности и необходимости установления политики и целей информационной безопасности;

– реализации и эксплуатации средств управления с точки зрения управления всеми рисками бизнеса организации;

– контроля и анализа рабочих характеристик и эффективности СМИБ;

– постоянного совершенствования, основанного на объективных измерениях.

Модель, известная как модель "Планирование-Работа-Проверка-Действие" (PDCA), может быть применима ко всем процессам СМИБ. На рисунке 3 показано, как использовать СМИБ для введения требований к ИБ и ожиданий организаций электросвязи и заинтересованных сторон, связанных со сферой электросвязи, и как путем необходимых действий и процессов создать выходные продукты информационной безопасности (т. е. управляемую информационную безопасность), которые соответствуют этим требованиям и ожиданиям.

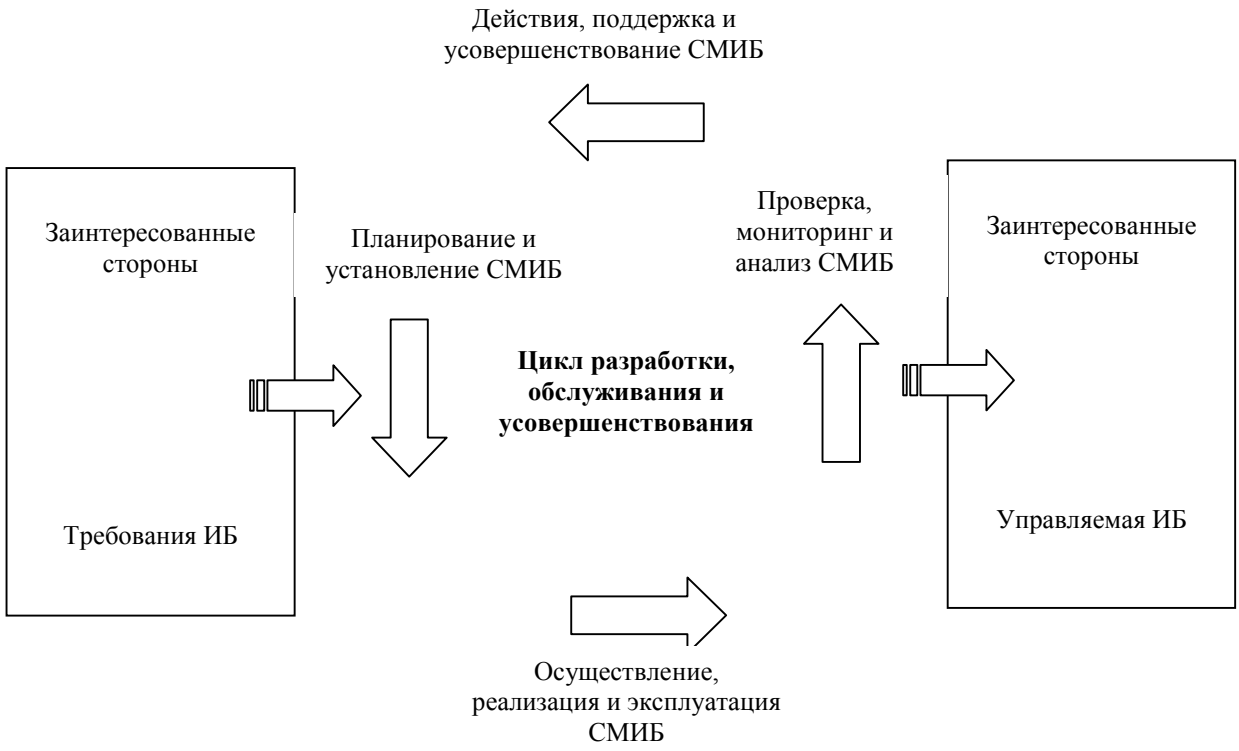

Рисунок 5 - Модель СМИБ

Планирование и установление СМИБ создает политику безопасности, цели, задачи, процессы и процедуры, соответствующие управляемым рискам и улучшенной информационной безопасности, для представления результатов в соответствии с общей политикой и целями организации.

Осуществление, реализация и эксплуатация СМИБ реализует и применяет политику безопасности, средства управления, процессы и процедуры.

Проверка, мониторинг и анализ СМИБ — оценка и, где это применимо, измерение рабочих характеристик процесса, относящегося к политике, целям безопасности и практическому опыту, и представление отчета о результатах в систему управления для анализа.

Действия, поддержка и усовершенствование СМИБ — принятие корректирующих и превентивных действий, основанных на результатах анализа руководством, для достижения непрерывных усовершенствований СМИБ.

Контрольные вопросы

1. Подход на котором должна основываться система менеджмента информационной безопасности связан с учетом рисков

основной деятельности организации электросвязи (бизнес-рисков) или только рисков нарушений информационной безопасности?

2. Как реализуется рабочий цикл модели СМИБ: однократно, регулярно через определенные интервалы времени или циклически непрерывно?

3. Что такое управляемая информационная безопасность?

4. Для функционирования СМИБ необходимо чтобы вся деятельность организации электросвязи была формализована на основе процессного подхода или только деятельность по управлению ИБ?

3.2 Процессы системы менеджмента информационной безопасности

Организация должна разрабатывать, реализовывать, поддерживать и непрерывно совершенствовать документированную СМИБ с позиции всей деловой деятельности и риска организации.

Процессы СМИБ.

Создание СМИБ. Организация должна:

– определить область применения СМИБ;

– определить политику СМИБ;

– определить системный подход к определению риска;

– идентифицировать риски;

– количественно определить риски;

– идентифицировать и оценить варианты обработки рисков;

– выбрать цели управления и средства управления для обработки рисков;

– подготовить заявление о применимости;

– получить согласие руководства на предлагаемые остаточные риски и разрешение на реализацию и эксплуатацию СМИБ.

Реализация и эксплуатация СМИБ. Организация должна:

– представить и реализовать план обработки риска;

– реализовать средства управления;

– обеспечить повышение квалификации и информированность персонала;

– управлять эксплуатацией;

– управлять ресурсами;

– реализовать процедуры.

Мониторинг и анализ СМИБ. Организация должна:

– выполнять процедуры мониторинга;

– проводить регулярные анализы;

– анализировать уровень остаточного риска;

– осуществлять внутренний аудит СМИБ;

– предпринять анализ системы руководством;

– регистрировать действия и события, которые могли бы повлиять на рабочие характеристики и эффективность СМИБ.

Поддержание и совершенствование СМИБ. Организация должна:

– реализовывать любые сформулированные усовершенствования СМИБ;

– предпринимать любые сформулированные исправляющие и профилактические действия;

– сообщать их результаты всем заинтересованным сторонам;

– проверять соответствие этих усовершенствований поставленным целям и задачам.

Контрольные вопросы и задания

1. К какой стадии и какому процессу может относиться установка в реальной телекоммуникационной системе программно-аппаратных средств защиты?
2. Какие действия применительно к СМИБ и почему более эффективны: корректирующие или профилактические?
3. Учитывая то, что выходные данные одного процесса непосредственно образуют входные данные следующего процесса, постройте возможную замкнутую модель СМИБ для перечисленных выше процессов для заданной организации.

3.3 Система документации. Ответственность руководства, менеджмент ресурсов. Обучение, осознание, компетенция

Организация должна иметь систему документации для СМИБ. В этой системе документы должны соответствующим образом защищаться и проверяться. Эта система должна также охватывать любые записи, которые создаются или сохраняются для образования доказательств эффективной работы СМИБ.

Руководство должно представить обоснования его обязательств по созданию, реализации, эксплуатации, контролю, анализу, поддержанию и совершенствованию СМИБ.

Организация должна определять и предоставлять ресурсы, необходимые для:

– создания, реализации, эксплуатации и поддержания СМИБ;

– гарантирования, что процедуры политики информационной безопасности поддерживают требования бизнеса;

– определения правовых и нормативных требований и обязательств по контрактам, а также обращения к ним;

– поддержки достаточной безопасности путем правильного применения всех реализованных средств управления;

– производства, при необходимости, анализов и соответственного реагирования на результаты этих анализов;

– повышения, при необходимости, эффективности СМИБ.

Организации следует обеспечить, чтобы весь персонал, которому назначены обязанности, определенные в СМИБ, являлся компетентным для выполнения требуемых задач. Организации также следует обеспечить, чтобы весь соответствующий персонал осознавал необходимость и важность своих действий по ИБ, а также то, как они могут содействовать обеспечению целей СМИБ.

Контрольные вопросы

1. Что может выступать в качестве обоснований обязательств руководства организации электросвязи по созданию, реализации, эксплуатации, контролю, анализу, поддержанию и совершенствованию СМИБ?
2. Кому и для чего должны представляться обоснования обязательств руководства организации электросвязи по созданию, реализации, эксплуатации, контролю, анализу, поддержанию и совершенствованию СМИБ?
3. Какие ресурсы могут быть необходимы для гарантирования того, что процедуры политики информационной безопасности поддерживают требования бизнеса

3.4 Анализ СМИБ, осуществляемый руководством. Внутренний аудит. Усовершенствование СМИБ

Руководство через запланированные периоды времени должно анализировать СМИБ организации, чтобы постоянно гарантировать ее соответствие, достаточность и эффективность. Подробнее эти требования изложены в ГОСТ Р ИСО/МЭК 27001.

Входные данные для анализа руководством должны содержать информацию о:

– результатах аудиторских проверок и анализов СМИБ;

– ответных реакциях заинтересованных сторон;

– методах, изделиях или процедурах, предназначенных для улучшения рабочих характеристик и эффективности СМИБ;

– статусе профилактических и исправляющих действий;

– уязвимостях и угрозах, недостаточно учтенных при предыдущем определении риска;

– мероприятиях, проведенных по результатам предыдущих анализов;

– любых изменениях, которые могли бы повлиять на СМИБ;

– рекомендациях по усовершенствованию.

Выходные данные анализа руководством должны содержать любые решения и действия, относящиеся к:

– повышению эффективности СМИБ;

– изменению процедур, влияющих на информационную безопасность, что необходимо в ответ на внутренние и внешние события, которые могут повлиять на СМИБ;

– потребностям в ресурсах.

Организация должна через запланированные интервалы проводить внутренний аудит СМИБ, чтобы определить цели контроля, средства контроля, процессы и процедуры для СМИБ.

Организация должна непрерывно повышать эффективность СМИБ.

Организация должна предпринимать действия по исключению случаев несоответствия в реализации и функционировании СМИБ, чтобы предотвратить их повторное возникновение.

Организация должна определить действия по защите от будущих несоответствий с целью предотвращения их появления.

Контрольные вопросы

1. Как можно оценить достаточность СМИБ и ее эффективность? В чем могут быть отличия этих показателей?
2. Почему ставятся условия непрерывного повышения эффективности СМИБ и исключения и предотвращения несоответствий СМИБ, но отсутствуют требования к изменению ее достаточности? Необходимы ли такие требования и как они могли бы быть сформулированы?
3. Кто может являться заинтересованными сторонами в эффективном функционировании СМИБ и в чем могут заключаться их ответные реакции?

3.5 Совокупность средств управления информационной безопасностью, ориентированных на требования для электросвязи

Цели управления средствами управления, перечисленными ниже, основаны на содержащихся в ГОСТ Р ИСО/МЭК 17799 и ГОСТ Р ИСО/МЭК 27001 требованиях. Они адаптированы к требованиям электросвязи. Список средств управления является исчерпывающим, но организации следует также рассматривать другие средства управления, описанные в ГОСТ Р ИСО/МЭК 17799 и ГОСТ Р ИСО/МЭК 27001. Цели управления и средства управления выбираются как часть процессов СМИБ, определенных выше.

3.5.1 Организационные меры безопасности: организационная инфраструктура ИБ, распределение обязанностей по обеспечению ИБ

Целью создания организационной инфраструктуры ИБ является управление ИБ в пределах организации электросвязи.

Структуру управления следует создавать так, чтобы она способствовала инициализации и осуществлению контроля за внедрением ИБ в организации электросвязи. Следует создавать соответствующие управляющие советы с участием высшего руководства для утверждения политики ИБ, назначать ответственных лиц в области ИБ, а также осуществлять координацию и внедрение мероприятий по управлению ИБ в организации электросвязи. При необходимости следует предусмотреть наличие специалиста по вопросам ИБ внутри организации электросвязи, к которому могут обращаться заинтересованные сотрудники. Следует налаживать контакты с внешними специалистами по безопасности для того, чтобы быть в курсе отраслевых тенденций, способов и методов ее оценки, а также с целью адекватного реагирования на инциденты нарушения ИБ. Следует поощрять многопрофильный подход к ИБ, например, путем налаживания сотрудничества между менеджерами, пользователями, администраторами, разработчиками приложений, аудиторами и сотрудниками безопасности, а также специалистами в области страхования и управления рисками.

Ответственность за защиту отдельных средств электросвязи и за выполнение конкретных процессов, обеспечивающих безопасность, должна быть четко определена.

Линейные администраторы технического обслуживания сети являются ответственными за обеспечение безопасности каждого коммутатора электросвязи, как определяется конкретной политикой

безопасности. Администратор (менеджер) технического обслуживания сети ответственен за:

– обеспечение того, чтобы пользовательские терминалы системы технического обслуживания сети были расположены в закрытой зоне, как описано в политике и процедурах обеспечения физической безопасности;

– обеспечение того, чтобы регистрации пользователей коммутируемого доступа и регистрации идентификаторов пользователей были соответствующим образом установлены и поддерживались;

– обеспечение того, чтобы разрешительные коды службы коммутации центральной станции применялись соответствующим образом;

– поддержку мер безопасности, гарантирующих, что доступ к коммутаторам электросвязи находится под контролем.

3.5.2 Менеджмент активов. Ответственность за активы: идентификация активов, владение активами

Целью является достижение и поддержание защиты активов электросвязи.

Каждый актив должен быть четко идентифицирован; должна быть проведена и поддерживаться инвентаризация всех важных активов.

Организация электросвязи должна идентифицировать все активы и задокументировать важность этих активов.

Должна быть проведена и поддерживаться инвентаризация важных активов, относящихся к каждой организации электросвязи. Существует много типов активов, относящихся к организации электросвязи, в том числе:

– средства коммутации: коммутаторы для телефонной связи, Интернета и подвижной связи, которые управляют информацией маршрутизации, информацией об абонентах, информацией "черных списков", зарегистрированной служебной информацией и т. п.;

– средства передачи: передающие ретрансляционные системы, сетевые кабели;

– эксплуатационные средства: системы управления электросвязью для эксплуатации средств коммутации и передачи, которые содержат эксплуатационную информацию, информацию о повреждениях, информацию о конфигурации, информацию о клиентах, информацию о денежных расчетах, статистическую информацию о трафике и т. п.;

– средства служб электросвязи: информационные службы порталов, службы вызовов в кредит и по предоплате, службы через оператора,

служба ADSL, "почтовая" служба, служба построения Web, служба подвижной связи, служба роуминга, служба подвижной "почтовой" связи, службы вызова по номеру/справочная служба и т. п.;

– люди, их квалификация и способности;

– нематериальные средства, такие как репутация и имидж организации.

С целью учета каждый актив должен иметь назначенного владельца.

Термин "владелец" означает лицо или сообщество, которое обладает утвержденной руководством ответственностью за управление услугами электросвязи, техническое обслуживание, использование средств электросвязи и доступ к ним. Термин "владелец" не подразумевает, что данное лицо действительно обладает каким-либо правом собственности на средство. Владение может быть распределено в соответствии с:

– бизнес-процессом;

– определенной совокупностью действий;

– приложением/службой;

– определенным набором данных.

3.5.3 Менеджмент активов. Классификация информации: руководящие принципы классификации, маркировка и обработка информации

Целью классификации является получение информационными активами защиты соответствующего уровня.

Информация и выходные данные из систем, обрабатывающих классифицируемые данные, должны классифицироваться с точки зрения их ценности, конфиденциальности и критичности для организации электросвязи.

Классификация и связанные с ней защитные средства управления для информации должны учитывать потребности бизнеса в информации совместного или ограниченного пользования и последствия для бизнеса, связанные с такими потребностями.

Указания по классификации должны содержать соглашения по начальной классификации и повторной классификации через некоторое время в соответствии с некоторой предварительно определенной методикой.

Классификация информационных активов может быть выполнена с точки зрения их конфиденциальности, целостности и доступности или любого другого критерия, подходящего для выражения потребностей в защите.

Информация, связанная с абонентами и клиентами, должна обрабатываться с учетом ее конфиденциальности. Информация, относящаяся к средствам коммутации и передачи, также должна управляться с учетом ее критичности.

В соответствии со схемой классификации, утвержденной в организации электросвязи, должна быть разработана соответствующая совокупность процедур для маркировки и обработки информации.

Процедуры маркировки информации необходимы для размещения информационных активов в физическом и электронном форматах.

Выходные данные систем, содержащих информацию, которая классифицируется как конфиденциальная или критичная, должны нести соответствующую классификационную метку (на выходе).

Для каждого уровня классификации должны быть определены процедуры обработки, охватывающие безопасную обработку, хранение, передачу, переклассификацию и уничтожение. Сюда должны быть включены также процедуры регистрации любого события, относящегося к безопасности.

Соглашения с другими органами электросвязи, которые содержат положения о совместном использовании информации, должны содержать процедуры для определения классификации такой информации и для опознавания классификационных меток от других органов электросвязи.

3.5.4 Вопросы безопасности, связанные с персоналом. Информирование об инцидентах и нарушениях ИБ: информирование об инцидентах безопасности, информирование о проблемах безопасности, информирование о сбоях ПО, обучение на инцидентах

Целью является минимизация вреда от инцидентов и нарушений безопасности, контроль таких инцидентов и обучение на примере инцидентов.

Об инцидентах безопасности должно быть сообщено как можно быстрее по каналам управления электросвязью.

Об инцидентах безопасности, вызванных различными типами угроз, такими как вирусы, "троянские кони", черви, злонамеренные коды подвижной связи, должно быть немедленно сообщено соответствующим служащим и контрагентам с использованием формальной процедуры извещения.

После извещения об инциденте должна быть правильно выполнена процедура ответа об инциденте.

Для минимизации вреда, наносимого устройствам и службам электросвязи в результате инцидента, должны быть выполнены ответные процессы восстановления. При необходимости, следует также сразу известить об инциденте соответствующих клиентов по прямой электронной почте и/или на домашнюю страницу, предоставляемую организацией электросвязи.

Пользователям информационных служб должна быть направлена просьба обращать внимание и сообщать о любых замеченных подозрительно слабых местах безопасности или об угрозах системам или службам.

Организация электросвязи должна хорошо знать конфигурацию системы и спецификации с точки зрения безопасности и должна проявлять заботу о слабых местах и/или уязвимости системы безопасности.

Если обнаружено слабое место, то о нем следует сообщить соответствующему руководству для поддержания системы в безопасном состоянии.

Должны выполняться процедуры сообщения об отказе программного обеспечения.

Должны выполняться процедуры извещения об отказе программного обеспечения в системе электросвязи. Необходимо предусмотреть следующие действия:

– обращать внимание на признаки проблемы и любые сообщения, появляющиеся в системе управления электросвязью;

– систему электросвязи, если это возможно, следует изолировать, а ее использование прекратить. Надо немедленно проинформировать соответствующее контактное лицо. Если систему надо проверить, то ее следует отсоединить от любой работающей сети электросвязи, прежде чем запустить;

– о событии следует немедленно сообщить менеджеру по информационной безопасности;

– восстановление должно выполняться соответствующим обученным и опытным персоналом.

Должны иметься механизмы, способные оценивать и контролировать типы, количество и стоимость инцидентов и нарушений.

Эту информацию следует использовать для опознавания повторных или сильно влияющих инцидентов или нарушений.

3.5.5 Физическая безопасность и защита от окружающей среды. Зоны безопасности: периметр физической безопасности, физические средства управления доступом

Цель является предотвращение несанкционированного физического доступа, ущерба и воздействий в отношении помещений и безопасности информации организации.

Объект электросвязи должен использовать периметры безопасности (такие ограждения, как стены, контролируемые с помощью карточек проходные или посты с человеком) для защиты зон, в которых размещаются устройства коммутации, передачи, эксплуатации и обработки информации.

По отношению к периметрам физической безопасности должны учитываться и реализовываться, по возможности, следующие руководящие указания:

– периметры безопасности должны быть четко определены, а местоположение и прочность каждого периметра должны зависеть от требований к безопасности средств, находящихся внутри периметра, и результатов определения риска;

– физическая безопасность является ключевой задачей в средствах электросвязи, она должна быть эффективно решена с тщательным соблюдением всех локальных политик безопасности, чтобы гарантировать постоянную защиту корпоративных средств. Если система функционирует неправильно, или политика не соблюдается, то необходимо немедленно решить этот вопрос;

– по периметру здания или территории, содержащих средства обработки информации, должна быть установлена звуковая сигнализация (т. е. не должно быть брешей в периметре или зонах, где мог бы легко произойти прорыв). Внешние стены объекта должны иметь прочную конструкцию, а все внешние двери должны быть соответствующим образом защищены от несанкционированного доступа управляемыми механизмами, например, засовами, тревожной сигнализацией, замками и т. п. Двери и окна должны запираться, а для окон, в особенности расположенных на первом этаже, должна быть предусмотрена необслуживаемая и наружная защита. В особенности надежно такими управляемыми механизмами должны быть защищены периметры базовых станций подвижной связи, которые расположены в отдельных зонах;

– для контроля физического доступа на территорию или в здание должен иметься пост с человеком или другие средства. Доступ на участок или в здания должен быть открыт только уполномоченному персоналу;

– физические барьеры, где это возможно, должны располагаться от пола до потолка, чтобы предотвратить несанкционированный вход и загрязнение из окружающей среды;

– все пожарные двери по периметру безопасности должны быть оборудованы тревожной сигнализацией, контролироваться и запираться при захлопывании;

– должны быть установлены подходящие системы обнаружения вторжения, соответствующие национальным, региональным или международным стандартам. Должен регулярно проверяться охват этими системами всех наружных дверей и доступных окон;

– эксплуатационные центры электросвязи должны быть оборудованы надежными системами обнаружения физического вторжения. Незанятые зоны должны постоянно контролироваться средствами тревожной сигнализации. Должен быть обеспечен также охват других зон, например вычислительных залов или комнат для общения;

– устройства обработки информации, управляемые объектами электросвязи, должны быть физически отделены от устройств обработки, управляемых посторонним объектом;

– устройства, принадлежащие организациям электросвязи, например, передающие устройства, устройства коммутации и инфраструктуры электросвязи, должны быть физически отделены от других устройств, например, устройств клиентов в управляемом центре данных.

Зоны безопасности должны быть защищены с помощью соответствующих средств контроля входа, чтобы гарантировать, что доступ получит только уполномоченный персонал.

Должны учитываться следующие руководящие принципы:

– посетители зон безопасности должны находиться под наблюдением или иметь допуск, а дата и время их прибытия и убытия должны быть записаны. Они должны иметь разрешенный доступ только к конкретным, санкционированным вопросам и должны быть снабжены инструкциями о требованиях к безопасности в данной зоне и о процедурах, проводимых в чрезвычайных ситуациях;

– на посту пропуска информация о других посетителях должна быть защищена. Например, даты и время их прибытия и убытия не должны располагаться в легко просматриваемом месте. Принимающее лицо должно также проверить вещи посетителя на предмет наличия в них опасных объектов;

– доступ в зоны, в которых обрабатывается конфиденциальная информация и в которых находятся устройства обработки информации, должен контролироваться и разрешаться только для уполномоченных лиц. Для разрешения и подтверждения любого доступа должны использоваться средства контроля аутентификации, например, карты управления доступом плюс PIN-код. В особенности, механизмом строгого контроля входа должны быть достаточно защищены рабочие комнаты с работающими средствами;

– контрольный журнал всех доступов должен обрабатываться с соблюдением мер безопасности;

– надо требовать, чтобы весь персонал был одет в некую форму с видимой идентификацией, и должно поощряться выявление несопровождаемых посторонних лиц и лиц, не носящих видимой идентификации;

– персонал вспомогательных служб третьей стороны должен иметь право ограниченного доступа в зоны безопасности или к устройствам обработки конфиденциальной информации только в случаях, когда это требуется. Этот доступ должен быть разрешенным и контролируемым;

– права доступа в зоны безопасности должны регулярно пересматриваться и обновляться;

– оператор электросвязи должен иметь контракт с соответствующей компанией обеспечения безопасности для физической защиты конфиденциальных устройств электросвязи. При обнаружении несанкционированного физического доступа оператор должен немедленно установить контакт со службой обеспечения безопасности по поводу этого инцидента.

3.5.6 Физическая безопасность и защита от окружающей среды. Зоны безопасности: защита зданий, производственных помещений и оборудования

Организация электросвязи должна проектировать и применять дополнительные меры физической безопасности для защиты офисов, помещений и устройств от порчи, вызываемой пожарами, наводнениями, землетрясениями, взрывами, гражданскими волнениями и другими формами природных или искусственных бедствий.

Должны быть учтены любые угрозы безопасности, исходящие от соседних помещений, например, должны быть учтены: пожар в соседнем здании, протечка воды с крыши или на этажи, расположенные ниже уровня земли, либо произошедший на улице взрыв.

При обеспечении безопасности офисов, помещений и устройств должны быть учтены следующие общие принципы:

– ключевые средства должны быть расположены так, чтобы исключить доступ к ним публики;

– там, где это возможно, здания не должны привлекать внимания, должны иметь минимальную индикацию об их назначении, не иметь слишком явной символики вне или внутри зданий, указывающих на проведение деятельности по обработке информации;

– справочники и внутренние телефонные книги, в которых указывается местоположение устройств, обрабатывающих конфиденциальную информацию, не должны быть легко доступны публике;

– опасные или легко воспламеняющиеся материалы должны храниться в охраняемом месте на безопасном расстоянии от зоны безопасности. Большие запасы материалов, таких как канцелярские товары, не должны храниться в зоне безопасности, если они не требуются;

– запасное оборудование и резервные носители информации должны размещаться на безопасном расстоянии, чтобы избежать порчи от бедствия на главном участке.

Для устройств электросвязи должны учитываться следующие специальные средства:

– обеспечение безопасности центров связи. Для защиты средств связи, таких как устройства коммутации, обеспечивающие электросвязь (называемые далее "центрами связи"), должно выполняться следующее:

– для размещения центров связи должны выбираться твердые участки земли. При необходимости, может быть выбран менее твердый участок, но должны быть приняты достаточные меры, чтобы предупредить неровное оседание;

– для размещения центров связи должны выбираться участки, окружающая среда которых наименее подвержена ущербу от ветра, воды и т. п. При необходимости, может быть выбран менее удовлетворительный участок, но должны быть приняты меры защиты от разрушений, вызываемых ветром, водой и т. п.;

– для размещения центров связи должны выбираться участки, окружающая среда которых наименее подвержена влиянию сильного электромагнитного поля. При необходимости, может быть выбран менее удовлетворительный участок, но должны быть приняты меры

для защиты помещений с оборудованием электросвязи при помощи электромагнитных экранов и т. п.;

– для размещения центров связи не следует использовать участки, смежные с сооружениями, в которых хранятся опасные вещества, которые создают опасность взрыва или возгорания;

– здания для центров связи должны иметь сейсмостойкую конструкцию;

– здания для центров связи должны иметь огнеупорную или огнестойкую конструкцию;

– здания для центров связи должны иметь требуемую конструктивную прочность в части нагрузки на пол;

– в центрах связи везде, где это необходимо, должна быть установлена автоматическая пожарная сигнализация;

– в центрах связи везде, где это необходимо, должны быть установлены огнетушители;

– обеспечение безопасности помещения с оборудованием электросвязи. Для защиты помещения, в котором установлены средства связи, обеспечивающие электросвязь (называемого далее "помещением с оборудованием электросвязи"), должны учитываться следующие средства управления:

– помещение с оборудованием электросвязи должно располагаться там, где наименее возможны внешние воздействия, такие как природные бедствия;

– помещение с оборудованием электросвязи должно располагаться там, где наименее возможно вторжение неуполномоченного персонала. Это не обязательно, если принимаются достаточные меры, чтобы предотвратить подобные вторжения;

– помещение с оборудованием электросвязи должно располагаться там, где наименее возможны наводнения. Если это помещение должно располагаться там, где наводнения возможны, то должны быть приняты необходимые меры, такие как подъем уровня пола, установление преград для проникновения воды или установка специальных устройств для дренажа воды;

– помещение с оборудованием электросвязи должно располагаться там, где наименее возможен ущерб от сильного

электромагнитного поля. Если это помещение должно находиться там, где электромагнитное поле возможно, то оно должно быть защищено электромагнитным экраном или как-нибудь иначе;

– важные устройства должны быть размещены в особом помещении с оборудованием электросвязи, имеющим двери достаточной прочности;

– должны быть приняты меры по предотвращению обрушения и падения материалов, используемых для полов, стен, потолков и т. п., при землетрясениях с нормальной, предсказуемой амплитудой;

– материалы, используемые для полов, стен, потолков и т. п., должны быть невоспламеняющимися или огнестойкими;

– должны быть приняты меры, позволяющие справиться со статическим электричеством;

– если средства электропитания установлены в помещении с оборудованием электросвязи, то должны быть приняты необходимые меры по предотвращению помех от электромагнитного поля;

– в помещениях с оборудованием электросвязи должны быть спроектированы сквозные отверстия для проверки распространения огня;

– при необходимости, должны быть приняты меры по защите помещения с хранилищем данных и сейфа с данными от электромагнитного воздействия;

– при необходимости, должны быть приняты меры по обеспечению огнестойкости помещения с хранилищем данных и выделенного склада;

– везде, где необходимо, в помещении с оборудованием электросвязи, в помещении с оборудованием кондиционирования воздуха и т. п. должна быть установлена автоматическая пожарная сигнализация;

– везде, где необходимо, в помещении с оборудованием электросвязи, в помещении с оборудованием кондиционирования воздуха и т. п. должны быть установлены огнетушители;

– в помещении с оборудованием электросвязи должно производиться необходимое кондиционирование воздуха;

– кондиционирование воздуха в помещении с оборудованием электросвязи, в котором располагаются важные устройства, должно осуществляться системой, отделенной от той, которая делает это в офисах и других помещениях. Это может быть необязательным, если приняты достаточные меры для должного кондиционирования воздуха в помещении с оборудованием электросвязи;

– в управляемом центре данных информация о клиентах должна быть надлежащим образом защищена, если в нем установлены системы нескольких компаний, работающих в одной отрасли. Эти системы должны размещаться на разных этажах или местах;

– физически изолированная рабочая зона. Для защиты физически изолированной рабочей зоны (например, базовой станции подвижной связи), в которой установлены средства связи, обеспечивающие электросвязь (называемой далее "изолированной рабочей зоной"), должны учитываться следующие средства управления:

– изолированная рабочая зона должна обладать сейсмостойкостью, соответствующей обязательным национальным или региональным стандартам;

– изолированная рабочая зона должна быть оборудована средствами автоматического пожаротушения;

– изолированная рабочая зона должна контролироваться из удаленного офиса с целью обнаружения отказов оборудования, отказов электропитания, пожаров, недопустимой влажности и температуры и т. п.;

– охрана безопасности должна быть физически обеспечена надлежащими средствами, такими как ограда для перекрытия изолированной рабочей зоны. Поскольку обычно работа идет в необслуживаемом режиме, зона должна быть оснащена функцией автоматической тревожной сигнализации в центр технического обслуживания при появлении какого-либо инцидента.

3.5.7 Физическая безопасность и защита от окружающей среды. Зоны безопасности: работа в зонах безопасности, изолированные зоны доставки и погрузки материальных ценностей

Для предотвращения компрометации конфиденциальной информации и других активов, находящихся в зоне безопасности, должны быть учтены дополнительные средства управления.

При работе в зонах безопасности должны учитываться следующие основные принципы:

– персонал должен быть осведомлен о существовании или о деятельности в зоне безопасности только на основе принципа "знать то, что необходимо";

– неконтролируемая работа в зонах безопасности должна быть исключена как для соблюдения техники безопасности, так и для предотвращения возможности злонамеренных действий;

– незанятые зоны безопасности должны быть физически заперты и должны периодически проверяться;

– не разрешается использование фото, видео, аудио или другого записывающего оборудования без специальной санкции;

– персонал вспомогательных служб третьей стороны должен иметь право ограниченной работы в зонах безопасности только когда потребуется. Этот доступ должен быть разрешенным и контролируемым.

Зоны доставки и погрузки должны контролироваться и, если возможно, изолироваться от устройств обработки информации во избежание несанкционированного доступа.

Должны учитываться следующие руководящие указания:

– доступ в зону доставки и погрузки снаружи здания должен быть разрешен только идентифицированному и уполномоченному персоналу;

– зона доставки и погрузки должна быть спроектирована так, чтобы поставляемые материалы могли бы быть разгружены без участия персонала доставки, имеющего доступ к другим частям здания;

– наружная(ые) дверь(и) зоны доставки и погрузки должны быть заперты, когда внутренняя дверь открыта;

– входящий материал должен быть проверен на наличие потенциальной угрозы до его перемещения из зоны доставки и погрузки в пункт использования;

– входящий материал, если это уместно, должен быть зарегистрирован на входе в участок.

3.5.8 Физическая безопасность и защита от окружающей среды. Безопасность оборудования: расположение и защита оборудования, безопасность вспомогательного оборудования

Цель: предотвратить потери, повреждение или компрометацию средств, а также прерывание деловой деятельности.

Оборудование должно быть размещено или защищено для уменьшения рисков окружающих угроз и возможностей несанкционированного доступа.

Для защиты оборудования должны учитываться следующие руководящие указания:

– оборудование должно быть размещено так, чтобы минимизировать ненужный доступ в рабочие зоны;

– средства электросвязи, обрабатывающие конфиденциальные данные, должны располагаться так, чтобы уменьшить риск того, что информация будет видна неуполномоченным лицам во время ее использования;

– устройства, требующие специальной защиты, должны быть изолированы, чтобы понизить общий уровень необходимой защиты;

– должны быть утверждены средства управления для минимизации риска потенциальных физических угроз, например, краж, пожаров, взрывов, задымления, воды (или аварии водоснабжения), пыли, вибрации, химических воздействий, помех по электропитанию, помех по линиям связи, электромагнитного излучения, вандализма. В частности, оборудование электросвязи должно быть выполнено и устойчиво размещено для обеспечения стойкости при землетрясениях. Для защиты от грозы должен устанавливаться грозозащитный трансформатор.

– организация должна предусмотреть указания, касающиеся возможности еды, питья и курения вблизи средств электросвязи;

– окружающие условия должны контролироваться в тех случаях, когда они могут неблагоприятно повлиять на работу средств электросвязи;

– защита от молний должна быть осуществлена во всех зданиях, а молниезащитные фильтры должны быть установлены на всех входящих силовых линиях и линиях связи;

– должно учитываться влияние любого бедствия, возникающего в соседних помещениях, например, пожара в соседнем здании, протечки воды с крыши или на этажах, расположенных ниже уровня земли, или взрыва на улице.

Оборудование должно быть защищено от аварий электроснабжения и других нарушений, вызванных вспомогательными средствами.

Все вспомогательные средства, такие как электроснабжение, водоснабжение, канализация, отопление/вентиляция и кондиционирование воздуха, должны регулярно осматриваться и, если нужно, тестироваться, чтобы обеспечить их правильное функционирование и уменьшить любой риск, вызванный их неправильной работой или отказом.

В отношении вспомогательных систем должны учитываться следующие руководящие указания:

– для оборудования, поддерживающего критические деловые операции, рекомендуется с целью обеспечения непрерывной работы или плановых прекращений работы использовать источники бесперебойного электропитания (ИБП). Планы для аварийных ситуаций с электроснабжением должны предусматривать действия на случай отказа ИБП. Оборудование ИБП должно регулярно проверяться, чтобы гарантировать, что оно имеет достаточную мощность и соответствует требованиям электросвязи, особенно для центров управления;

– если обработка должна продолжаться в случае продолжительного перерыва в электроснабжении, то должен быть предусмотрен резервный генератор. Если генератор установлен, он должен регулярно проверяться на соответствие инструкциям по электросвязи. Должны иметься достаточные запасы топлива, чтобы обеспечить работу генератора в течение длительного времени;

– аварийные выключатели электропитания должны располагаться вблизи аварийных выходов помещений, в которых размещено оборудование, чтобы облегчить быстрое выключение энергии при аварийной ситуации. На случай отказа основного источника питания должно быть обеспечено аварийное освещение;

– в частности, электрические устройства в изолированных зонах, таких как базовые станции подвижной связи, должны иметь возможность обеспечивать мощность, достаточную для всех нагрузок. Если это невозможно, то на месте уязвимости должен быть установлен следящий механизм для зарядной емкости. Для защиты от отказов электропитания должна устанавливаться аккумуляторная батарея. В изолированной зоне мощность батареи должна быть особенно повышенной, либо должен быть установлен собственный электрический генератор достаточной мощности.

3.5.9 Физическая безопасность и защита от окружающей среды. Безопасность оборудования: безопасность кабельной системы, обслуживание оборудования

Система силовых кабелей электросвязи, переносящих данные или обслуживающих информационные службы, должна быть защищена от перехвата или повреждения.

Для обеспечения безопасности кабельных систем должны учитываться следующие руководящие указания:

– силовые линии и линии электросвязи, идущие к средствам обработки информации, должны находиться под землей или под полом, где это возможно, либо иметь достаточную другую защиту;

– система сетевых кабелей должна быть защищена от несанкционированного перехвата или повреждения, например, путем использования кабелепровода или путем обхода зон общего пользования;

– силовые кабели, во избежание помех, должны быть отделены от кабелей связи;

– для конфиденциальных или критичных систем рассматриваются дополнительные средства управления:

  – установка бронированного кабелепровода и организация запертых помещений или коробок в пунктах осмотра или окончания;

  – использование разных трасс или передающих сред, обеспечивающих соответствующую безопасность;

  – использование волоконно-оптических кабелей;

  – использование электромагнитного экранирования для защиты кабелей;

  – организация технического зондирования и физических инспекций для обнаружения несанкционированных устройств, подключенных к кабелям.

Чтобы гарантировать готовность и целостность, оборудование должно правильно технически обслуживаться.

При техническом обслуживании оборудования должны учитываться следующие руководящие указания:

– оборудование должно технически обслуживаться в соответствии со служебными интервалами и спецификациями, рекомендованными поставщиком;

– выполнять ремонт и обслуживать должен только уполномоченный персонал технического обслуживания;

– записи должны содержать все потенциальные или действительные отказы и все случаи профилактического и восстанавливающего технического обслуживания;

– должны быть предусмотрены соответствующие средства управления для обслуживания передающего оборудования, расположенного вне помещений, особенно в части удаленных, стертых и измененных данных. Должны выполняться все требования, налагаемые страховыми полисами.

3.5.10 Физическая безопасность и защита от окружающей среды. Безопасность оборудования: обеспечение безопасности оборудования, используемого вне помещений организации, безопасная утилизация или повторное использование оборудования

Безопасность, обеспечиваемая для оборудования, расположенного вне помещения, должна быть эквивалентной той, которой обладает оборудование, расположенное в помещении и используемое для той же цели, с учетом рисков работы вне помещений электросвязи.

Невзирая на право собственности, использование для обработки информации какого-либо оборудования, расположенного вне помещений электросвязи, должно быть санкционировано руководством.

Должны учитываться следующие руководящие указания по защите оборудования вне помещений:

– оборудование и носители информации, находящиеся вне помещений, не должны оставаться без присмотра в местах общего пользования. Портативные компьютеры должны переноситься как ручная кладь и маскироваться, где это возможно;

– инструкции производителя по защите оборудования, например, по защите от воздействия сильных электромагнитных полей, должны соблюдаться постоянно;

– средства контроля надомной работы должны быть установлены с помощью определения риска и подходящих средств управления, применяемых соответствующим образом, например, запирающиеся картотеки, правило "чистого стола", контроль доступа к компьютерам и безопасная связь с офисом;

– для защиты оборудования, расположенного вне помещения, должна иметься достаточная страховка;

– риски безопасности, например, от повреждения, кражи и подслушивания, в разных местах могут значительно отличаться, что

должно учитываться при определении наиболее подходящих средств управления.

Все виды оборудования, содержащего носители информации, например, фиксированные жесткие диски, должны быть проверены, чтобы гарантировать, что любые конфиденциальные данные и лицензионное программное обеспечение удалено или затерто до передачи.

Устройства, содержащие конфиденциальную информацию, должны быть физически разрушены, либо информация на них должна быть разрушена, удалена или затерта с использованием утвержденных методов, которые предпочтительнее стандартных функций удаления или форматирования.

3.5.11 Общие требования: правила "чистого стола" и "чистого экрана", вынос имущества

Цель общих требований - предотвратить компрометацию или кражу информации и средств обработки информации.

Объект электросвязи должен учитывать применение правила "чистого стола" по отношению к бумагам и переносимым накопителям-носителям, а к средствам обработки информации – правила "чистого экрана".

Правила "чистого стола/чистого экрана" уменьшают риск несанкционированного доступа, потерь и повреждения информации в обычное рабочее время и вне его. Информация, оставленная на столах, может быть повреждена и разрушена также в результате бедствия, такого как пожар, землетрясение, наводнение или взрыв.

Должны учитываться следующие руководящие указания:

– бумаги и компьютерные носители, когда они не используются, особенно в нерабочие часы, должны храниться в подходящих запираемых шкафах и/или в безопасной мебели другого типа;

– конфиденциальная или критичная деловая информация, когда она не требуется, в особенности, когда офис или помещение, в котором расположены средства, не заняты, должна быть заперта (идеально, в сейф, либо в шкаф, защищающий от физического ущерба);

– персональные компьютеры, компьютерные терминалы и печатающие устройства, не участвующие в работе, не следует оставлять зарегистрированными в системе, когда они не используются, они должны быть защищены с помощью закрываемых на ключ замков, паролей или других средств управления;

– пункты приема и выдачи электронных почтовых сообщений и необслуживаемые факсимильные аппараты должны быть защищены;

– должно быть предотвращено несанкционированное использование фотокопировальных устройств;

– конфиденциальная или классифицированная информация после печати должна немедленно удаляться из печатающих устройств.

Оборудование, информация или программное обеспечение не должны выноситься с объекта без разрешения.

Должны учитываться следующие руководящие указания:

– имущество не следует выносить с объекта без разрешения;

– должны быть четко определены лица, имеющие право разрешать вынос имущества из объекта;

– когда необходимо и уместно, оборудование должно быть снято с учета и вновь зарегистрировано при возвращении;

– для обнаружения несанкционированного выноса имущества должны производиться внезапные проверки;

– люди должны знать, что практикуются внезапные проверки.

3.5.12 Управление связью и эксплуатацией: эксплуатационные процедуры и ответственность за инфраструктуру информационной безопасности

Цель: гарантировать правильную и безопасную эксплуатацию средств обработки информации.

Чтобы гарантировать быструю, эффективную и упорядоченную реакцию на инциденты безопасности, а также для сбора относящихся к инциденту данных, таких как контрольные журналы и записи регистраций, должны быть установлены ответственность и процедуры управления при инциденте.

Должны учитываться следующие руководящие указания:

– следует устанавливать процедуры, охватывающие все возможные типы инцидентов безопасности, включая:

  – отказы системы электросвязи и прекращение обслуживания;

  – отказ в обслуживании;

  – ошибки, вызванные неполными или неточными деловыми данными;

  – изъяны в конфиденциальности;

– в дополнение к обычным планам на случай непредвиденных ситуаций (предназначенных для максимально быстрого восстановления систем или служб), указанными процедурами следует также охватывать:

– анализ и идентификацию причин инцидента;

– при необходимости, планирование и реализацию мер для предотвращения его повторного появления;

– сбор данных контрольных журналов и аналогичных сведений;

– взаимосвязь с данными, которые были вызваны восстановлением после инцидента или были привлечены для восстановления;

– извещение соответствующего руководства о действиях.

– следует собирать и подходящим способом засекречивать контрольные журналы и аналогичные сведения для:

– анализа внутренних проблем;

– использования в качестве свидетельств о потенциальных изъянах в контракте, изъянах в нормативных требованиях, либо в статье гражданского или уголовного кодекса;

– переговоров о компенсации от поставщика программного обеспечения или поставщика службы;

– поставленные клиентами вопросы, относящиеся к эксплуатации существующих клиентских конфигураций, такие как выход из строя аппаратуры, сетевые проблемы и т. п., а также относящиеся к конфигурациям компании, которые влияют на клиента и на работников, должны размещаться по некоторой шкале. Все клиенты должны быть полностью осведомлены о процедурах организации клиентской шкалы и иметь подходящую для них документацию. Например, поставленным клиентами вопросам могут быть присвоены приоритеты согласно установленным критериям:

– приоритет 1 (П1) – клиентский пункт полностью отказал или не способен выполнять требования соглашения об уровне обслуживания ;

– приоритет 2 (П2) – клиентский пункт значительно поврежден в результате неисправности; отказала одна система или более, либо наблюдается значительная потеря и/или задержка пакетов;

– приоритет 3 (П3) – ухудшение обслуживания клиента;

– приоритет 4 (П4) – запросы клиентов;

– приоритет 5 (П5) – прекращение рассмотрения.

Действия по ликвидации изъянов в безопасности и по исправлению отказов системы должны тщательно и официально управляться. Эти процедуры должны гарантировать, что:

– только четко определенный и уполномоченный персонал допускается к действующим системам и данным;

– все чрезвычайные действия должны подробно документироваться;

– о чрезвычайных действиях докладывается руководству и они рассматриваются в установленном порядке;

– целостность систем электросвязи и средств управления подтверждается с минимальной задержкой.

3.5.13 Управление связью и эксплуатацией: разделение экспериментальных и эксплуатационных средств, внешнее управление средствами

Экспериментальные и испытательные средства должны быть отделены от средств, находящихся в эксплуатации. Должны быть определены и документально оформлены правила перехода программного обеспечения из экспериментального статуса в эксплуатационный.

Экспериментальные и испытательные действия могут привести к непреднамеренным изменениям программного обеспечения и информации, если они совместно используют одну и ту же вычислительную среду. Поэтому желательно разделять экспериментальные, испытательные и эксплуатационные средства, чтобы снизить риск случайного изменения или несанкционированного доступа к эксплуатационному программному обеспечению и деловым данным. Должны учитываться следующие средства управления:

– экспериментальные и эксплуатационные программы должны выполняться, по возможности, на разных вычислительных процессорах, либо в разных доменах или директориях;

– экспериментальные и испытательные действия должны быть разделены как можно полнее;

– желательно, чтобы компиляторы, редакторы и другие системные утилиты не были доступны эксплуатационным системам, когда они не требуются;

– для уменьшения риска ошибок должны использоваться различные процедуры входа в эксплуатационную и испытательную системы;

– только персонал разработчика должен иметь доступ к эксплуатационным паролям, когда имеются средства управления,

вводящие пароли для поддержки эксплуатационных систем. Средства контроля должны гарантировать, что такие пароли изменяются после применения.

Прежде чем использовать службы внешнего управления средствами, должны быть определены риски, а соответствующие средства управления должны быть согласованы с подрядчиком и включены в договор.

Использование для управления средствами электросвязи внешнего подрядчика может привести к потенциальной незащищенности, такой как возможность компрометации, ущерба или потери данных на объекте подрядчика. Эти риски должны быть определены заранее, а соответствующие средства управления должны быть согласованы с подрядчиком и включены в договор.

3.5.14 Управление связью и эксплуатацией: защита от вредоносного программного обеспечения

Цель: защитить целостность программного обеспечения и информации от ущерба из-за вредоносного программного обеспечения.

Для защиты от вредоносного программного обеспечения и выполнения соответствующих процедур уведомления пользователя должны быть реализованы средства обнаружения и предотвращения.

Защита от вредоносного программного обеспечения должна основываться на уведомлениях о безопасности, на соответствующем доступе к системе и средствах управления изменениями. Должны учитываться следующие средства управления:

– когда программное обеспечение установлено, должна быть проведена оценка его качества;

– когда программное обеспечение или данные изменяются, в программном обеспечении должны быть приняты меры по предотвращению ошибок;

– программные отказы должны немедленно обнаруживаться; должно указываться место, в котором они появились.

3.5.15 Управление связью и эксплуатацией: организационная работа

Цель: обеспечить целостность и готовность служб электросвязи.

Регулярно должны делаться и тестироваться резервные копии важной информации и программного обеспечения электросвязи.

Должны быть предусмотрены достаточные резервные средства, чтобы гарантировать, что вся важная информация и программное

обеспечение электросвязи могут быть восстановлены после бедствия или отказа носителя. Резервные средства отдельных систем должны регулярно проверяться, чтобы гарантировать, что они соответствует требованиям непрерывного ведения бизнеса. Должны учитываться следующие руководящие указания:

– минимальный объем резервной информации, вместе с точными и полными записями резервных копий и задокументированными процедурами восстановления, должны храниться в месте, удаленном на достаточное расстояние, чтобы избежать любого ущерба от бедствия на главном объекте. По крайней мере, три поколения или цикла резервной информации должны сохраняться для важных деловых приложений и услуг;

– резервная информация должна быть представлена на соответствующем уровне физической защиты и защиты от окружающей среды, указанном в стандартах, применяемых на главном объекте. Средства управления, применяемые к носителям на главном объекте, должны быть расширены для охвата резервного объекта;

– резервные носители должны, по возможности, регулярно проверяться, чтобы гарантировать, что им можно доверять, когда потребуется их использовать при чрезвычайной ситуации;

– процедуры восстановления должны регулярно проверяться и испытываться, чтобы гарантировать, что они работают эффективно и что они могут быть завершены за время, отведенное в эксплуатационных процедурах на восстановление;

– должен быть определен срок хранения для важной информации электросвязи, а также определены требования к архивным копиям, которые хранятся постоянно.

Эксплуатационный персонал должен вести журнал своих действий. Журналы операторов должны быть объектами регулярных независимых проверок.

Журналы должны содержать, при необходимости:

– время начала и время завершения работы системы;

– подробные описания ошибок в системе и принимаемых в ответ на них исправляющих действий;

– подтверждение правильности обработки файлов данных и правильности выходных сигналов системы;

– имя лица, делающего запись в журнале.

Об отказах должно сообщаться и должны предприниматься действия по исправлению.

Следует регистрировать касающиеся систем электросвязи отказы, о которых сообщают пользователи.

Следует иметь четкие правила обработки сообщений об отказах, в том числе:

– просмотр записей об отказах, чтобы гарантировать, что они удовлетворительно преодолены;

– просмотр исправляющих мер, чтобы гарантировать, что средства управления не были скомпрометированы, а предпринятые действия полностью санкционированы.

3.5.16 Управление связью и эксплуатацией: общее управление (менеджмент) сети

Цель: гарантировать сохранность информации в сетях и защиту поддерживающей инфраструктуры.

Чтобы достичь и поддерживать безопасность в сетях, должен быть реализован ряд средств управления.

Для обеспечения безопасности в сетях электросвязи необходимо применять следующие восстанавливающие средства управления:

– передающие средства, такие как кабели передачи, должны хорошо технически обслуживаться. В случае чрезвычайной ситуации эти средства должны ремонтироваться как можно быстрее;

– коммутационные средства служб электросвязи должны хорошо технически обслуживаться, а их трафик должен постоянно контролироваться. В случае чрезвычайной ситуации эти средства должны быть немедленно переключены на резервные средства или другие маршруты, чтобы избежать серьезной перегрузки трафиком;

– в случае атак "отказ в обслуживании" (DoS) коммутационные средства, такие как маршрутизаторы, должны обрабатывать больший объем трафика по сравнению с обычной ситуацией. Одной из функций средств управления должно быть ограничение трафика до приемлемого уровня.

3.5.17 Управление доступом: требования бизнеса электросвязи к управлению доступом

Цель: управлять доступом к информации.

Должны быть определены и задокументированы требования бизнеса электросвязи к управлению доступом, а доступ должен быть ограничен так, как определено политикой управлением доступом.

В политике управления доступом должны быть четко сформулированы правила и права управления доступом для каждого пользователя или группы пользователей электросвязи. Следует четко уведомить пользователей и поставщиков служб о требованиях бизнеса электросвязи, которым должны удовлетворять средства управления доступом.

В данной политике необходимо учитывать следующее:

– требования к безопасности отдельных приложений бизнеса электросвязи;

– идентификация всей информации, относящейся к приложениям бизнеса;

– политика распространения и авторизации информации, например, необходимость знать принципы и уровни безопасности, а также классификацию информации;

– согласованность стратегий управления доступом и классификации информации различных систем и сетей;

– соответствующие юридические нормы и любые договорные обязательства, касающиеся защиты доступа к данным или услугам.

3.5.18 Управление доступом: управление доступом к приложениям

Цель: предотвратить несанкционированный доступ к информационным приложениям, содержащимся в информационных системах.

Доступ к информации и к прикладным функциям системы должен быть ограничен согласно политике управления доступом.

Ограничения доступа должны быть основаны на отдельных требованиях к приложению бизнеса электросвязи. Политика управления доступом должна быть также согласована с политикой доступа, действующей в организации электросвязи.

Конфиденциальные системы должны иметь выделенную (изолированную) вычислительную среду.

При изоляции конфиденциальной системы должны быть учтены следующие аспекты:

– конфиденциальность прикладной системы должна быть установлена и задокументирована владельцем этого приложения;

– конфиденциальные системы, такие как база данных клиента, должны выполняться на изолированном компьютере, а совместно

использовать ресурсы с доверенными прикладными системами должны только по договоренности с владельцем конфиденциального приложения.

3.5.19 Разработка и техническое обслуживание системы: требования к безопасности систем электросвязи

Цель: гарантировать, что средства обеспечения безопасности встроены в системы электросвязи.

Требования к бизнесу электросвязи для новых систем или для усовершенствования существующих систем должны определять требования к средствам управления.

Требования к безопасности и средства управления должны отражать ценность для бизнеса участвующих массивов информации и потенциальный ущерб бизнесу, который может быть причинен в случае отказа или отсутствия безопасности.

Системные требования к информационной безопасности и процессы реализации безопасности должны объединяться на ранних этапах проектирования информационной системы.

Структура анализа требований к безопасности и определения средств управления, их удовлетворяющих, основывается на определении риска и управлении риском.

3.5.20 Разработка и техническое обслуживание системы: безопасность в приложениях

Цель: предотвратить потери, несанкционированное изменение или неправильное использование данных в прикладных системах.

Следует проверять правильность входных данных приложений, чтобы гарантировать их правильность и уместность.

Проверки должны применяться к вводу деловых транзакций, постоянных данных (например, имен и адресов клиентов, кредитных лимитов, справочных номеров клиентов) и таблиц параметров (например, ставка платы за разговор, курс обмена валюты, ставки налогов).

Выходные данные приложений должны проверяться на правильность, чтобы гарантировать, что обработка накопленной информации ведется правильно и соответствует обстоятельствам.

Проверка правильности выходных данных должна охватывать:

– проверки правдоподобности с целью определения обоснованности выходных данных;

– предоставление достаточной информации для читателя или для последующей системы обработки, чтобы определять правильность, полноту, точность и классификацию этой информации;

– процедуры ответа на проверку правильности выходных данных.

3.5.21 Разработка и техническое обслуживание системы: криптографические средства управления

Цель: защитить конфиденциальность, аутентичность или целостность информации.

Организация электросвязи должна разработать политику применения ею криптографических средств управления для защиты ее информации.

При разработке политики должны рассматриваться следующие вопросы:

– подход системы управления к использованию криптографических средств управления во всей организации электросвязи;

– подход к управлению ключами, включая методы защиты криптографических ключей и восстановления зашифрованной информации в случае потери, компрометации или повреждения ключей;

– роли и ответственность за реализацию криптографической политики;

– как должен определяться подходящий уровень криптографической защиты;

– влияние применения зашифрованной информации на средства управления, использующие методы сканирования содержимого (например, обнаружение вируса во время связи).

Шифрование должно применяться для защиты конфиденциальности конфиденциальной или критичной информации.

Следует установить необходимый уровень защиты, основываясь на определении риска и учитывая тип и качество используемого алгоритма шифрования, а также длины применяемых криптографических ключей. При реализации криптографической политики следует учитывать нормы и национальные ограничения, которые могут повлиять на применение криптографических методов в различных частях света и на пропуск трансграничных потоков зашифрованной информации. Кроме того, следует провести рассмотрение руководящих документов, которые применяются к экспорту и импорту криптографической технологии.

Управление ключами должно применяться для обеспечения использования криптографических методов в электросвязи.

Все ключи должны быть защищены от изменений и разрушений, а секретные и личные ключи нуждаются в защите от несанкционированного раскрытия. Для защиты оборудования, используемого для генерирования, хранения и архивирования ключей, должна быть использована физическая защита.

Содержимое соглашений об уровне обслуживания или договоров с внешними поставщиками криптографических услуг, например, с органом сертификации, должно охватывать вопросы ответственности и надежности служб, а также время ответа при предоставлении услуг.

3.5.22 Разработка и техническое обслуживание системы: безопасность системных файлов

Цель: для обеспечения безопасности доступ к системным файлам должен контролироваться.

Необходимы процедуры для управления реализацией программного обеспечения в эксплуатационных системах.

Для минимизации риска нарушения работы эксплуатационных систем должны учитываться следующие руководящие указания:

– обновление эксплуатационного программного обеспечения, приложений и библиотек программ должно выполняться только обученными администраторами, имеющими соответствующее разрешение в системе управления;

– программное обеспечение приложений и операционных систем должно включаться в работу только после обширного, достаточного и успешного тестирования. Если они должны быть применены в таких чувствительных системах, как коммутационные средства, то тест должен выполняться с полным охватом всех частей;

– все обновления библиотек эксплуатационных программ должны быть зарегистрированы в контрольном журнале;

– предыдущие версии прикладного программного обеспечения должны сохраняться на непредвиденный случай. В случае программного обеспечения конфиденциального приложения должны храниться, по крайней мере, три поколения программного обеспечения;

– старые версии программного обеспечения должны архивироваться вместе со всей необходимой информацией и параметрами, процедурами, деталями конфигурации и с поддерживающим программным обеспечением;

– любое решение об обновлении к новой версии должно учитывать безопасность этой версии, т. е. введение новой функциональной

возможности безопасности или количество и строгость проблем безопасности, затрагивающих эту версию;

– в программном обеспечении должны применяться "заплаты", если они могут помочь устранить или уменьшить слабые места безопасности.

Данные тестирования должны быть защищены и должны контролироваться.

При тестировании данных должно быть исключено использование эксплуатационных данных, содержащих личную информацию или любую другую конфиденциальную информацию. Если для тестирования используется личная или конфиденциальная информация, то все конфиденциальные детали и содержимое должны быть удалены или изменены до неузнаваемости перед началом тестирования.

Для защиты эксплуатационных данных, используемых для целей тестирования, должны применяться следующие руководящие указания:

– процедуры управления доступом, которые применяются к эксплуатационным прикладным системам, должны применяться также к тестовым прикладным системам;

– отдельная авторизация должна производиться каждый раз, когда эксплуатационная информация копируется в тестовую прикладную систему;

– эксплуатационная информация должна быть обязательно стерта из тестовой прикладной системы сразу после завершения тестирования.

Должен осуществляться строгий контроль доступа к библиотеке текстов программ.

Для уменьшения вероятности порчи компьютерных программ должны учитываться следующие требования к контролю доступа к библиотекам текстов программ:

– библиотеки текстов программ не должны храниться в эксплуатационных системах;

– персонал, поддерживающий информационные технологии для средств электросвязи, не должен иметь неограниченный доступ к библиотекам текстов программ;

– программы, которые разрабатываются или технически обслуживаются, не должны содержаться в библиотеке текстов эксплуатационных программ. Эти программы должны храниться в разрабатываемых или технически обслуживаемых средствах;

– в контрольном журнале должны производиться записи обо всех доступах к библиотекам текстов программ;

– техническое обслуживание и копирование библиотек текстов программ должно быть объектом строгих процедур контроля изменений.

3.5.23 Разработка и техническое обслуживание системы: безопасность процессов разработки и поддержки

Цель: поддержка безопасности программного обеспечения и информации прикладной системы.

Реализация изменений должна строго контролироваться пользователем формальной процедуры контроля изменений.

Формальные процедуры контроля изменений в системах электросвязи должны быть строго задокументированы и введены в действие, чтобы минимизировать порчу информационных систем.

Введение новых систем и большие изменения в существующих системах должны сопровождаться формальными процессами документирования, спецификации, тестирования, контроля качества, а также управляемой реализацией.

Этот процесс должен охватывать определение риска, анализ влияний изменений и спецификацию необходимых средств управления безопасностью.

Этот процесс должен содержать:

– необходимые изменения, представленные уполномоченными пользователями;

– проверку средств управления процедурами обеспечения целостности, чтобы убедиться, что они не скомпрометированы этими изменениями;

– выявление всего компьютерного программного обеспечения, информации, объектов баз данных и аппаратных средств, требующих изменения;

– получение формального одобрения детализированных предложений до начала работы;

– гарантию того, что уполномоченный пользователь согласился с изменениями до их реализации;

– гарантию того, что набор системной документации обновляется после завершения каждого изменения и что старая документация архивируется или уничтожается;

– поддержание контроля номера версии при всех обновлениях программного обеспечения;

– поддержание контрольного журнала всех запросов на изменение;

– гарантию того, что изменения реализуются в нужное время и не мешают затронутым процессам бизнеса электросвязи.

После изменений прикладные системы должны быть осмотрены и протестированы.

Этот процесс должен охватывать:

– проверку прикладных процедур управления и обеспечения целостности, чтобы гарантировать, что они не скомпрометированы изменениями в операционной системе;

– гарантию того, что уведомление об изменениях операционной системы выдано вовремя, что позволяет провести соответствующие тесты и осмотры до реализации изменений.

Средства управления должны быть применимы к безопасной разработке программного обеспечения сторонними силами.

Следующие аспекты должны учитываться в случаях, когда разработка программного обеспечения выполняется сторонними силами:

– лицензионные положения, право собственности на программу и права интеллектуальной собственности;

– сертификация качества и правильности выполненной работы;

– условное соглашение с третьей стороной на случай ошибки третьей стороны;

– права доступа для проверки качества и точности выполненной работы;

– договорные требования к качеству программы;

– тестирование перед установкой с целью выявления вредоносной программы.

Контрольные вопросы и задания

1. За обеспечение безопасности каждого коммутатора электросвязи отвечают специалисты по безопасности или линейные администраторы технического обслуживания сети? Где документируется подобное распределение обязанностей по безопасности?
2. Кто в организации электросвязи может быть назначен владельцем нематериальных средств, таких как репутация и имидж организации?
3. Что может служить критериями, подходящими для выражения потребностей в защите, при классификации информационных активов?
4. Предложите возможные механизмы, способные оценивать стоимость инцидентов и нарушений.

5. Почему физическая безопасность является ключевой задачей для средств электросвязи?
6. Оцените, насколько это возможно, соответствие защищенности известных региональных «центров связи" описанным выше требованиям.
7. Поясните смысл требования о том, что зона доставки и погрузки должна быть спроектирована так, чтобы поставляемые материалы могли бы быть разгружены без участия персонала доставки, имеющего доступ к другим частям здания.
8. Какими могут быть возможные указания организации электросвязи, относительно возможности еды, питья и курения вблизи средств электросвязи?
9. Почему силовые кабели должны быть отделены от кабелей связи?
10. От каких угроз безопасности должно быть защищено оборудование, расположенное вне помещений организации электросвязи?
11. Правила "чистого стола/чистого экрана" в организации электросвязи должны использоваться в рабочее время, в нерабочее время или постоянно?
12. С какой целью должны приоритезироваться в соответствии со специальной шкалой поставленные клиентами вопросы, относящиеся к эксплуатации существующих клиентских конфигураций, такие как выход из строя аппаратуры, сетевые проблемы?
13. Зачем необходимо разделять экспериментальные, испытательные и эксплуатационные средства в организации электросвязи?
14. Сколько поколений или циклов резервной информации должны сохраняться для важных деловых приложений и услуг?
15. Какие защитные меры должны быть предусмотрены для защиты от атак "отказ в обслуживании" (DoS) на такие коммутационные средства, как маршрутизаторы?
16. На чем должна основываться структура анализа требований к безопасности и определения средств управления, их удовлетворяющих?
17. Сколько поколений программного обеспечения конфиденциальных приложений необходимо сохранять в организации электросвязи?
18. Что понимается под управляемой реализацией при сопровождении введения новых систем и больших изменениях в существующих системах?

4 Защита от помех цифровых систем передачи информации

4.1 Основные характеристики цифровых систем связи

Достоверность передачи информации. Система связи должна обладать помехоустойчивостью, т.е. способностью восстанавливать с достаточной верностью переданное сообщение при приеме сигнала, искаженного помехой, поступающей от различного рода источников помех, как непреднамеренных, так и преднамеренных. При приеме цифровой информации регистрируется последовательность импульсов, составляющая кодовое слово. Если в результате воздействия помех принятое кодовое слово не будет соответствовать переданному, то получателю с выхода декодирующего устройства при простом кодировании выдается искаженное сообщение.

Для количественной оценки соответствия принятого сообщения переданному используют отношения чисел ошибочно принятых элементов сообщения $М_{ОШ}$ к общему числу переданных элементов $М_{ОБЩ}$

$$К_{ОШ} = \frac{М_{ОШ}}{М_{ОБЩ}}. \qquad (1)$$

Следует различать достоверность, обеспечиваемую каналом связи (на разряд), и системой связи (на кодовое слово или группу слов).

Отношение (1) называют частостью ошибок или коэффициентом ошибок. При ограниченном времени передачи величина $К_{ОШ}$ является случайной и зависит от этого времени. Однако если общее время передачи информации (сеанс связи) значительно и статистические характеристики процесса передачи при этом неизменны (стационарный канал связи), то величина $К_{ОШ}$ остается устойчивой и почти не меняется от сеанса к сеансу. Практически такие условия во многих случаях выполняются. Поэтому в первом приближении коэффициент ошибок можно считать близким к вероятности ошибки приема одного элемента сообщения p_1.

В связи с этим достоверность передачи цифровой информации, как правило, и оценивается величиной вероятности ошибочного приема p_1 одного элемента сообщения. Из-за своей простоты и удобства оценка качества передачи цифровой информации по допустимому значению p_1 нашла наиболее широкое применение.

Скорость передачи информации. При передаче цифровой информации различают два понятия скорости передачи: техническую и информационную.

Техническая скорость характеризует быстродействие аппаратуры, входящей в состав передающей части системы связи. Она определяется количеством элементов дискретного сообщения, переданных в секунду. Эта характеристика была предложена в телеграфии французским инженером Жаном Бодо. В его честь единица технической скорости названа бодом.

Техническая скорость передачи определяется величиной

$$B = \frac{1}{\tau_0} \text{ бод}, \qquad (2)$$

где τ_0 – длительность посылки одного элемента дискретного сообщения.

Техническую скорость передачи часто называют скоростью манипуляции (модуляции). Зная продолжительность единичного интервала τ_0, легко определить скорость манипуляции B и наоборот. Так, при B=1000 бод=1кбод → τ_0=1мс, или при τ_0=20 мс → B=50 бод.

Наряду с технической скоростью передачи, в теории информации широко применяются понятия информационной скорости передачи и пропускной способности канала связи. Под информационной скоростью понимают количество информации, поступившее по линии связи от источника информации к получателю за одну секунду. Информационная скорость измеряется числом двоичных единиц (бит) в секунду. Термин «бит» происходит от английского названия двоичной единицы – *binary digit*. Скорость передачи информации зависит от целого ряда факторов: технической скорости передачи, статистических свойств источника, типа канала связи, применяемых сигналов, уровня помех и вида искажений сигналов в канале.

Потенциальные возможности канала характеризует его пропускная способность, которая определяется как верхняя граница (или максимум) скорости передачи информации.

Необходимо отметить отличие в понятиях пропускной способности канала (информационной скорости) и технической скорости (скорости манипуляции). Пропускная способность характеризует быстродействие канала с информационной точки зрения, а скорость манипуляции – технические возможности аппаратуры. Пропускная способность является основной характеристикой при решении задачи согласования канала связи с источником сообщений.

Конкретные значения скорости передачи цифровой информации и вероятности ошибки существенно зависят от типа канала связи, вида сигнала и его энергии, уровня помех в канале, требований к качеству передачи и т. п.

Так, при передаче команд, как правило, предъявляются очень высокие требования к достоверности и сравнительно невысокие требования к скорости передачи (вероятность искажения команды иногда не должна превышать $10^{-6} \div 10^{-8}$, а время передачи команды может быть значительным – порядка секунды). Дискретные команды в некоторых системах управления должны обладать высокой криптостойкостью (не поддаваться быстрой расшифровке) и имитостойкостью (обладать свойствами, затрудняющими повторение команд с целью нарушения нормальной работы управления).

При передаче цифровых последовательностей, полученных дискретизацией непрерывных сообщений, требования к достоверности передачи ниже, чем при передаче команд, и допустимая вероятность ошибки кодовой комбинации обычно составляет $10^{-3} \div 10^{-5}$. Зато требования к скорости передачи существенно выше, и скорость может достигать значений в десятки и сотни тысяч бит в секунду, а в современных цифровых системах связи доходит до десятков миллионов бит в секунду.

4.2 Основные параметры кодов

Коды характеризуются следующими основными параметрами.

Основание кода (модуль) m определяется числом отличающихся друг от друга символов в алфавите. Простейший число-импульсный унитарный код имеет алфавит, состоящий из одних единиц, и применяется, например в АТС для вызова абонента по телефону с помощью телефонного диска (номеронабирателя).

Все другие коды имеют алфавит, состоящий из двух ("0" и "1") и более символов, отличающихся друг от друга. Коды с основанием m=2 называются двоичными, с основанием m=3 – троичными и т.д. При использовании в процессе кодирования электрических импульсов значение m определяет число различных градаций их амплитуды, фазы, частоты или других так называемых избирающих признаков.

В системах связи двоичная система счисления и двоичные коды получили наиболее широкое применение, главным образом, из-за сравнительно простой аппаратурной реализации логических операций и арифметических действий, а также устройств для передачи, опознавания и запоминания сообщений.

Преобразование сообщения в сигнал при двухпозиционных кодах производится с помощью триггеров, которые могут находиться только в одном из двух устойчивых состояний: 0 и 1. Устройства с тремя

состояниями реализуются значительно сложнее, поэтому многоосновные коды с основанием $m>2$ применяются значительно реже.

Длина кодовой комбинации – n, называется разрядностью кода или длиной слова, *n* равно количеству символов (элементарных сигналов) в кодовой комбинации. Для конкретного заданного кода имеется свое множество (набор) кодовых комбинаций, каждая из которых соответствует передаче отдельного дискретного сообщения первичного алфавита источника сообщений. Код называется равномерным, если все кодовые комбинации одинаковы по длине ($n=const$), и неравномерным, если величина *n* в коде непостоянна ($n=var$).

Неравномерность в длине кодовых комбинаций усложняет построение автоматических преобразующих устройств, а также исключает возможность разделения кодовых комбинаций при их последовательном приеме без применения специальных разделительных символов между ними. Поэтому для упрощения работы декодирующих устройств предпочтительнее иметь одинаковое число элементов в каждой кодовой комбинации.

Число кодовых комбинаций – N в коде, каждая из которых может передавать свое отдельное сообщение. Значение *N* для кода с основанием *m* и числом элементов *n* определяется выражением

$$N = m^n. \qquad (3)$$

Совокупность кодовых комбинаций называется кодовым словарем.

Если все возможные комбинации *n*-элементного кода используются для кодирования сообщения, то такой первичный код называется полным, а также простым или обыкновенным (иногда такой код называют примитивным). Основным назначением первичных кодов является представление дискретной информации источника сообщений в цифровой форме.

Помимо первичных кодов в цифровых системах передачи информации находят применение корректирующие коды, позволяющие обнаруживать и исправлять ошибки, вызванные помехами в канале связи. В соответствии с этим корректирующие коды получили название – *помехоустойчивые коды*.

Сущность построения корректирующих (помехоустойчивых) кодов состоит в том, что из общего числа кодовых комбинаций *N*, которые можно получить при *n*-элементном коде (для двоичного кода $N=2^n$), для передачи сообщений выбирается меньшее число $N_0<N$ комбинаций, называемых *разрешенными*. Остальные $N–N_0$ комбинаций, называемые

з*апрещенными*, не используются для передачи сообщений, что приводит к избыточности в коде.

Избыточность кода, в котором используются только N_0 кодовых комбинаций из общего возможного числа N, характеризуется коэффициентом избыточности, определяемым выражением

$$\chi = 1 - \frac{\log_2 N_0}{\log_2 N} = 1 - \frac{n_0}{n} = \frac{n - n_0}{n}, \qquad (4)$$

где n – число разрядов данного кода; n_0 – число разрядов неизбыточного (полного) кода, у которого N_0 такое же, как у данного кода ($n>n_0$).

Коды, обладающие большей избыточностью, имеют и большую помехоустойчивость. Увеличение избыточности приводит к уменьшению пропускной способности системы связи, так как значительно возрастает число элементов m в кодовых комбинациях. Поэтому выбор кодов с определенными корректирующими возможностями, а следовательно, и с определенной избыточностью, должен быть всегда строго обоснован, исходя из характера распределения ошибок в канале связи и получения необходимой достоверности принимаемой информации.

Кодовое расстояние – d определяется количеством разрядов, в которых одна кодовая комбинация данного кода отличается от другой.

Для двоичного кода кодовое расстояние определяется количеством ненулевых разрядов при суммировании по модулю 2 двух сравниваемых кодовых комбинаций.

Пример. $d = 00101 \oplus 11110 = 11011$.

Минимальное кодовое расстояние – d_{min} равно наименьшему числу не совпадающих по значению одноименных разрядов при попарном сравнении всех N комбинаций кода. Для двоичного кода d_{min} – это наименьшее количество ненулевых разрядов в сумме по модулю 2 всех пар кодовых комбинаций. Впервые понятие кодового расстояния ввел в теорию кодирования Р. Хемминг, поэтому d_{min} называют хеммингговым расстоянием.

Для полных, простых кодов (3) всегда d_{min}=1.

Пример. $d = 00101 \oplus 00001 = 00100$.

Очевидно, что при построении корректирующего кода желательно выбирать разрешенные кодовые комбинации таким образом, чтобы хеммингговы расстояния между ними были как можно большими. Корректирующие коды могут обеспечивать решение задач обнаружения ошибок и исправления ошибок, возникших при передаче кодовых комбинаций по каналам связи.

Корректирующие возможности избыточных кодов полностью характеризуются именно величиной кодового расстояния d_{min}. Если код используется только для обнаружения ошибок кратностью $g_{ОБН}$, то необходимо и достаточно, чтобы

$$d_{min} \geq g_{ОБН} + 1. \qquad (5)$$

Кратностью ошибки g называют число позиций кодовой комбинации, на которых под действием помехи одни символы оказались замененными на другие, например 0 на 1 или 1 на 0. С учетом (5) условие обнаружения всех ошибок кратностью $g_{ОБН}$ записывается в виде

$$g_{ОБН} \leq d_{min} - 1. \qquad (6)$$

Чтобы можно было исправить все ошибки кратностью $g_{ИСПР}$ и менее, необходимо иметь большее минимальное расстояние, удовлетворяющее условию

$$d_{min} \geq 2 \cdot g_{ИСПР} + 1. \qquad (7)$$

В этом случае любая кодовая комбинация с числом ошибок g отличается от каждой разрешенной комбинации не менее, чем в $g+1$ позициях. Условие исправления всех ошибок кратностью не более $g_{ИСПР}$ можно записать в виде

$$g_{ИСПР} \leq \frac{d_{\min} - 1}{2}. \qquad (8)$$

Корректирующие коды можно одновременно использовать и для обнаружения и для исправления ошибок.

Вес кода (кодовой комбинации) – W определяется для двоичного кода количеством единиц в данной кодовой комбинации.

Пример.

Кодовая комбинация – 01111 – $W=4$.

Кодовая комбинация – 10000 – $W=1$.

Взвешенность кода – соответствие символов кода весовым коэффициентам системы счисления. Для любой системы счисления произвольное число N записывается в виде значений коэффициентов k_i ряда

$$N = \sum_{i=0}^{n-1} k_i \cdot m^i = k_{n-1} \cdot m^{n-1} + \ldots + k_1 \cdot m^1 + k_0 \cdot m^0, \qquad (9)$$

где N – число разрядов кода; k – весовой коэффициент ($0 \leq k_i \leq m-1$).

Если в основу правил соответствия кодовых комбинаций числам положены математические системы счисления (9), то такие коды называются арифметическими или взвешенными.

Примером взвешенного кода является натуральный двоичный код (НДК), в котором все кодовые комбинации соответствуют последовательности чисел десятичной системы счисления. Примером невзвешенного кода является рефлексный двоичный код (РДК) Грея.

4.3 Принципы помехоустойчивого кодирования

В реальных условиях прием двоичных символов всегда происходит с ошибками, когда вместо символа "1" принимается символ "0" и наоборот. Ошибки могут возникать из-за помех, действующих в канале связи (особенно помех импульсного характера), изменения за время передачи характеристик канала (например, замирания), снижения уровня передачи, нестабильности амплитудно- и фазочастотных характеристик канала и т. п.

Общепринятым критерием оценки качества передачи в дискретных каналах является нормированная на знак или символ допустимая вероятность ошибки для данного вида сообщений. Так, допустимая вероятность ошибки при телеграфной связи может составлять 10^{-3} (на знак), а при передаче данных – не более 10^{-6} (на символ). Для обеспечения таких значений вероятностей одного улучшения только качественных показателей канала связи может оказаться недостаточным. Поэтому основной мерой является применение специальных методов повышения качества приема передаваемой информации. Эти методы можно разбить на две группы.

К первой группе относятся методы увеличения помехоустойчивости приема единичных элементов (символов) дискретной информации, связанные с выбором уровня сигнала, отношения сигнал – помеха (энергетические характеристики), ширины полосы канала, методов приема и т. д.

Ко второй группе относятся методы обнаружения и исправления ошибок, основанные на искусственном введении избыточности в передаваемое сообщение. Увеличить избыточность передаваемого сигнала можно различными способами. Так как объем сигнала

$$V=P\cdot\Delta F\cdot T, \qquad (10)$$

где P – мощность сигнала, Вт; ΔF – ширина спектра сигнала, Гц; T – время передачи сигнала, с, то его увеличение возможно за счет увеличения P, ΔF и T.

Практические возможности увеличения избыточности за счет мощности и ширины спектра сигнала в системах передачи дискретной информации по стандартным каналам резко ограничены. Поэтому для повышения качества приема, как правило, идут по пути увеличения времени передачи и используют следующие основные способы:

- многократную передачу кодовых комбинаций (метод повторения);

- одновременную передачу кодовой комбинации по нескольким параллельно работающим каналам;

- помехоустойчивое (корректирующее) кодирование, т.е. использование кодов, исправляющих ошибки.

Иногда применяют комбинации этих способов.

Старейшим способом повышения достоверности в системах передачи является способ многократного повторения (дублирования) всего сообщения или его отдельных элементов. Многократное повторение (l раз) кодовой комбинации является самым простым способом повышения достоверности приема и легко реализуется, особенно в низкоскоростных системах передачи для каналов с быстро меняющимися параметрами. На приемном конце канала связи при этом применяется метод накопления повторяющихся посылок путем принятия решения о виде символа по "k" повторившимся значениям в процессе l-кратной передачи (метод "k" из "l") или по большинству принятых одноименных элементов (метод "голосования по большинству" или "мажоритарный метод").

Способу многократного повторения аналогичен способ передачи одной и той же информации по нескольким параллельным каналам связи.

В этом случае необходимо иметь не менее трех каналов связи (например, с частотным разнесением), несущие частоты которых нужно выбирать таким образом, чтобы ошибки в каналах были независимы. Достоинством таких систем являются надежность и малое время задержки в получении информации. Основным недостатком многоканальных систем так же, как и систем с повторением, является нерациональное использование избыточности.

Наиболее целесообразно избыточность используется при применении помехоустойчивых (корректирующих) кодов.

При помехоустойчивом кодировании чаще всего считают, что избыточность источника сообщений на входе кодера равна $\chi=0$. Это обусловлено тем, что очень многие дискретные источники (например, цифровая информация на выходе ЭВМ) обладают малой избыточностью. Если избыточность первичных источников сообщений существенна, то в этих случаях по возможности стремятся ее уменьшить путем эффективного кодирования, применяя, например коды Шеннона–Фано или Хаффмена. Затем методами помехоустойчивого кодирования можно внести такую избыточность в сигнал, которая позволит достаточно простыми средствами улучшить качество приема. Таким образом, эффективное кодирование вполне может сочетаться с помехоустойчивым.

В обычном равномерном непомехоустойчивом коде число разрядов n в кодовых комбинациях определяется числом сообщений и основанием кода.

Коды, у которых все кодовые комбинации разрешены к передаче, называются простыми или равнодоступными и являются полностью безызбыточными. Безызбыточные первичные коды обладают большой "чувствительностью" к помехам.

Внесение избыточности при использовании помехоустойчивых кодов обязательно связано с увеличением n–числа разрядов (длины) кодовой комбинации. Таким образом, все множество $N=2^n$ комбинаций можно разбить на два подмножества: подмножество разрешенных комбинаций, т.е. обладающих определенными признаками, и подмножество запрещенных комбинаций, этими признаками не обладающих.

Помехоустойчивый код отличается от обычного тем, что в канал передаются не все кодовые комбинации N, которые можно сформировать из имеющегося числа разрядов n, а только их часть N_k, которая составляет подмножество разрешенных комбинаций.

Если при приеме выясняется, что кодовая комбинация принадлежит к запрещенным, то это свидетельствует о наличии ошибок в комбинации, т.е. таким образом решается задача обнаружения ошибок. При этом принятая комбинация не декодируется (не принимается решение о переданном сообщении). В связи с этим помехоустойчивые коды называют корректирующими кодами. Корректирующие свойства избыточных кодов зависят от правила их построения, определяющего структуру кода, и параметров кода (длительности символов, числа разрядов, избыточности и т.п.).

Первые работы по корректирующим кодам принадлежат Хеммингу, который ввел понятие минимального кодового расстояния d_{min} и предложил код, позволяющий однозначно указать ту позицию в кодовой комбинации, где произошла ошибка. К информационным элементам k в коде Хемминга добавляется r проверочных элементов для автоматического определения местоположения ошибочного символа.

4.4 Классификация помехоустойчивых корректирующих кодов

Помехоустойчивые (корректирующие) коды делятся на блочные и непрерывные.

Блочными называются коды, в которых информационный поток символов разбивается на отрезки и каждый из них преобразуется в определенную последовательность (блок) кодовых символов. В блочных кодах кодирование при передаче (формирование проверочных элементов)

и декодирование при приеме (обнаружение и исправление ошибок) выполняются в пределах каждой кодовой комбинации (блока) в отдельности по соответствующим алгоритмам.

Непрерывные или *рекуррентные* коды образуют последовательность символов, не разделяемую на отдельные кодовые комбинации. Кодирование и декодирование непрерывно совершаются над последовательностью элементов без деления их на блоки. Формирование проверочных символов ведется по рекуррентным (возвратным) правилам, поэтому непрерывные коды часто называют рекуррентными или *цепными*.

В простейшем цепном коде каждый проверочный элемент формируется путем сложения по модулю 2 соседних или отстоящих друг от друга на определенное число позиций информационных элементов. В канал связи передается последовательность импульсов, в которой за каждым информационным следует проверочный. Подобную чередующуюся последовательность разрядов имеет, например корреляционный манчестерский код.

К непрерывным кодам относятся и сверточные коды, в которых каждый информационный символ, поступающий на вход кодирующего устройства, вызывает появление на его выходе ряда проверочных элементов, образованных суммированием по модулю 2 данного символа и k–1 предыдущих информационных символов. Рекуррентные коды позволяют исправлять групповые ошибки ("пачки") в каналах связи.

Блочные коды делятся на *равномерные* и *неравномерные*. В равномерных кодах, в отличие от неравномерных, все кодовые комбинации содержат одинаковое число n-символов (разрядов) с постоянной длительностью τ_0 импульсов символов кода. Равномерные коды в основном и применяются в системах связи, так как это упрощает технику передачи и приема.

Классическими примерами неравномерного кода являются код Морзе, широко применяемый в телеграфии, и код Хафмена, применяемый для компрессии информации (факсимильная связь, ЭВМ).

Никаких специальных мер по исправлению и обнаружению ошибок в коде Морзе не предусматривается в связи с большой избыточностью самого передаваемого текста. В этом смысле код Морзе не относится к классу корректирующих кодов.

Почти все блочные корректирующие коды принадлежат к *разделимым* кодам, в которых кодовые комбинации состоят из двух частей: информационной и проверочной. Их символы всегда занимают одни и те же позиции, т.е. располагаются на определенных местах. Как правило, в таких кодах, все кодовые комбинации которых содержат n

символов, первые k символов являются информационными, а за ними располагаются (n–k)-проверочных символов. В соответствии с этим разделимые коды получили условное обозначение – (n, k)-коды.

В *неразделимых* кодах деление на информационные и проверочные символы отсутствует. К таким кодам относятся, в частности, коды с постоянным весом, так называемые равновесные коды. Например, Международным союзом электросвязи (МСЭ-Т) рекомендован для использования телеграфный код № 3 (МТК№3) – семиразрядный код с постоянным весом, т.е. с числом единиц в каждой кодовой комбинации, равным 3 (W=3).

Систематические коды образуют наиболее обширную группу (n, k)-разделимых кодов. Особенностью этих кодов является то, что проверочные (корректирующие) символы образуются с помощью линейных операций над информационными. Кроме того, любая разрешенная кодовая комбинация может быть получена в результате линейной операции над набором k линейно независимых кодовых комбинаций. В частности, суммирование по модулю 2 двух и более разрешенных комбинаций также дает разрешенную кодовую комбинацию. Поскольку теоретической основой получения таких комбинаций является математический аппарат линейной алгебры, то коды и называют линейными, а учитывая, что проверочные символы формируются по определенной системе (правилам), блочные равномерные разделимые линейные коды получили название систематических. Использование аппарата линейной алгебры, в которой важное значение имеет понятие "группа", породило и другое название этих кодов – *групповые*.

Эти коды получили наибольшее применение в системах передачи дискретной информации.

Несистематические (*нелинейные*) коды указанными выше свойствами не обладают и применяются значительно реже в специальных случаях. Примером нелинейного кода является уже упоминавшийся неразделимый, равновесный код. Эти коды обычно используются в несимметричных каналах связи, в которых вероятность перехода 1→0 значительно больше вероятности перехода 0→1, или наоборот. В таких каналах очень маловероятно, чтобы в одном блоке были переходы обоих видов, и поэтому почти все ошибки приводят к изменению веса блока, и, следовательно, обнаруживаются.

Другим примером несистематического кода является код с контрольным суммированием – *итеративный* код. В этом коде проверочные разряды формируются в результате суммирования значений разрядов как в данной кодовой комбинации, так и одноименных разрядов в

ряде соседних с ней комбинаций, образующих совместный блок. Итеративные коды позволяют получить так называемые *мощные* коды, т.е. коды с длинными блоками и большим кодовым расстоянием при сравнительно простой процедуре декодирования. Итеративные коды могут строиться как комбинационные посредством произведения двух или более систематических кодов.

К комбинационным кодам можно отнести также *антифединговые* коды, предназначенные для обнаружения и исправления ошибок в каналах с замираниями (федингом) сигналов. Для таких каналов с группированием ошибок применяют метод *перемежения* символов или *декорреляции* ошибок. Он заключается в том, что символы, входящие в одну кодовую комбинацию, передаются не непосредственно друг за другом, а перемежаются символами других кодовых комбинаций исходного систематического или любого другого кода. Если интервал между символами, входящими в одну кодовую комбинацию, сделать длиннее "памяти" (интервала корреляции) канала с замираниями, то в пределах длительности одной исходной кодовой комбинации группирования ошибок не будет. На приеме после обратной "расфасовки" в кодовых комбинациях можно производить декодирование с обнаружением и исправлением ошибок.

В систематических кодах различают два метода формирования проверочной группы символов: *поэлементный* и *в целом*.

Наиболее известны среди систематических кодов коды Хемминга, которые исторически были найдены раньше многих других кодов и сыграли большую роль в развитии теории корректирующих кодов. В этих кодах используется принцип проверки на четность определенного ряда информационных символов. Проверочная группа из r символов формируется поэлементно по соответствующему алгоритму. Коды Хемминга, имеющие $d_{min}=3$, позволяют исправить одну ошибку.

Расширенные коды Хемминга строятся в результате дополнения кодов с $d_{min}=3$ общей проверкой каждой из кодовых комбинаций на четность, т.е. еще одним проверочным символом. Это позволяет увеличить минимальное кодовое расстояние до $d_{min}=4$.

Циклические коды также относятся к классу линейных систематических кодов и обладают всеми их свойствами. Коды названы циклическими потому, что циклический сдвиг любой разрешенной кодовой комбинации также является разрешенной комбинацией. Теория построения циклических кодов базируется на разделах высшей алгебры, изучающей свойства двоичных многочленов. Особую роль в этой теории играют так называемые неприводимые многочлены, т. е. полиномы,

которые не могут быть представлены в виде произведения многочленов низших степеней. В связи с этим циклические коды относят к разновидности *полиномиальных* кодов.

Среди циклических кодов особое место занимает класс кодов, предложенных Боузом и Рой–Чоудхури и независимо от них Хоквингемом. *Коды Боуза–Чоудхури–Хоквингема* получили сокращенное наименование *БЧХ-коды* и отличаются специальным выбором порождающего (образующего) циклический код полинома, что приводит к простой процедуре декодирования.

В циклических кодах r проверочных символов, добавляемых к исходным k информационным, могут быть получены сразу, т. е. в целом, в результате умножения исходной подлежащей передаче кодовой комбинации $Q(x)$ простого кода на одночлен x^r и добавлением к этому произведению остатка $R(x)$, полученного в результате деления произведения на порождающий полином P(x).

Отметим, что коды Хемминга также можно получить по алгоритмам формирования циклических кодов.

Проблема помехоустойчивого кодирования представляет собой обширную область теоретических и прикладных исследований. Основными задачами при этом являются следующие: отыскание кодов, эффективно исправляющих ошибки требуемого вида; нахождение методов кодирования и декодирования и простых способов их реализации.

Наиболее разработаны эти задачи применительно к систематическим кодам. Такие коды успешно применяются в вычислительной технике, различных автоматизированных цифровых устройствах и цифровых системах передачи информации.

4.5 Основные характеристики корректирующих кодов

В настоящее время наибольшее внимание с точки зрения технических приложений уделяется двоичным блочным корректирующим кодам.

При использовании блочных кодов цифровая информация передается в виде отдельных кодовых комбинаций (блоков) равной длины. Кодирование и декодирование каждого блока осуществляется независимо друг от друга.

Почти все блочные коды относятся к разделимым кодам, кодовые комбинации которых состоят из двух частей: информационной и проверочной. При общем числе n символов в блоке число информационных символов равно k, а число проверочных символов

$$r=n-k. \quad (11)$$

К основным характеристикам корректирующих кодов относятся:

— число разрешенных и запрещенных кодовых комбинаций;

— избыточность кода;

— минимальное кодовое расстояние;

— число обнаруживаемых или исправляемых ошибок;

— корректирующие возможности кодов.

Число разрешенных и запрещенных кодовых комбинаций. Для блочных двоичных кодов, с числом символов в блоках, равным n, общее число возможных кодовых комбинаций определяется значением

$$N_0=2^n. \quad (12)$$

Число разрешенных кодовых комбинаций при наличии k информационных разрядов в первичном коде:

$$N_k=2^k. \quad (13)$$

Очевидно, что число запрещенных комбинаций:

$$N_3=N_0-N_k=2^n-2^k, \quad (14)$$

а с учетом (11) отношение будет

$$\frac{N_0}{N_k}=\frac{2^n}{2^k}=2^{n-k}=2^r, \quad (15)$$

где r – число избыточных (проверочных) разрядов в блочном коде.

Избыточность корректирующего кода. Избыточностью корректирующего кода называют величину

$$\chi=\frac{r}{n}=\frac{n-k}{n}=1-\frac{k}{n}, \quad (16)$$

откуда следует

$$B_k=\frac{k}{n}=1-\chi. \quad (17)$$

Эта величина показывает, какую часть общего числа символов кодовой комбинации составляют информационные символы. В теории кодирования величину B_k называют *относительной скоростью кода*. Если производительность источника информации равна H символов в секунду, то скорость передачи после кодирования этой информации будет

$$B=H\frac{k}{n}, \quad (18)$$

поскольку в закодированной последовательности из каждых n символов только k символов являются информационными.

Если число ошибок, которые нужно обнаружить или исправить, значительно, то необходимо иметь код с большим числом проверочных символов. Чтобы при этом скорость передачи оставалась достаточно высокой, необходимо в каждом кодовом блоке одновременно увеличивать как общее число символов, так и число информационных символов. При этом длительность кодовых блоков будет существенно возрастать, что приведет к задержке информации при передаче и приеме. Чем сложнее кодирование, тем длительнее временная задержка информации.

Минимальное кодовое расстояние – d_{min}. Для того чтобы можно было обнаружить и исправлять ошибки, разрешенная комбинация должна как можно больше отличаться от запрещенной. Если ошибки в канале связи действуют независимо, то вероятность преобразования одной кодовой комбинации в другую будет тем меньше, чем большим числом символов они различаются.

Если интерпретировать кодовые комбинации как точки в пространстве, то отличие выражается в близости этих точек, т. е. в расстоянии между ними.

Количество разрядов (символов), которыми отличаются две кодовые комбинации, можно принять за кодовое расстояние между ними. Для определения этого расстояния нужно сложить две кодовые комбинации по модулю 2 и подсчитать число единиц в полученной сумме.

Заметим, что кодовое расстояние $d(x_i, x_0)$ между комбинацией x_i и нулевой x_0=00...0 называют весом W комбинации x_i, т. е. вес x_i равен числу "1" в ней.

Расстояние между различными комбинациями некоторого конкретного кода могут существенно отличаться. Так, в частности, в безызбыточном первичном натуральном коде (n=k) это расстояние для различных комбинаций может изменяться от единицы до величины n, равной значности кода. Особую важность для характеристики корректирующих свойств кода имеет *минимальное кодовое расстояние* d_{min}, определяемое при попарном сравнении всех кодовых комбинаций, которое называют расстоянием Хемминга.

В безызбыточном коде все комбинации являются разрешенными, и, следовательно, его минимальное кодовое расстояние равно единице – d_{min}=1. Поэтому достаточно исказиться одному символу, чтобы вместо переданной комбинации была принята другая разрешенная комбинация. Чтобы код обладал корректирующими свойствами, необходимо ввести в него некоторую избыточность, которая обеспечивала бы минимальное расстояние между любыми двумя разрешенными комбинациями не менее двух – $d_{min}\geq 2$.

Минимальное кодовое расстояние является важнейшей характеристикой помехоустойчивых кодов, указывающей на гарантируемое число обнаруживаемых или исправляемых заданным кодом ошибок.

Число обнаруживаемых или исправляемых ошибок. При применении двоичных кодов учитывают только дискретные искажения, при которых единица переходит в нуль (1→0) или нуль переходит в единицу (0→1). Переход 1→0 или 0→1 только в одном элементе кодовой комбинации называют *единичной ошибкой* (единичным искажением). В общем случае под *кратностью ошибки* подразумевают число позиций кодовой комбинации, на которых под действием помехи одни символы оказались замененными на другие. Возможны двукратные (g=2) и многократные (g>2) искажения элементов в кодовой комбинации в пределах $0 \le g \le n$.

Минимальное кодовое расстояние является основным параметром, характеризующим корректирующие способности данного кода. Если код используется только для обнаружения ошибок кратностью g_0, то необходимо и достаточно, чтобы минимальное кодовое расстояние было равно

$$d_{min} \ge g_0 + 1. \qquad (19)$$

В этом случае никакая комбинация из g_0 ошибок не может перевести одну разрешенную кодовую комбинацию в другую разрешенную. Таким образом, условие обнаружения всех ошибок кратностью g_0 можно записать

$$g_0 \le d_{min} - 1. \qquad (20)$$

Чтобы можно было исправить все ошибки кратностью $g_и$ и менее, необходимо иметь минимальное расстояние, удовлетворяющее условию

$$d_{min} \ge 2 \cdot g_и + 1. \qquad (21)$$

В этом случае любая кодовая комбинация с числом ошибок $g_и$ отличается от каждой разрешенной комбинации не менее чем в $g_и$+1 позициях. Если условие (21) не выполнено, возможен случай, когда ошибки кратности g исказят переданную комбинацию так, что она станет ближе к одной из разрешенных комбинаций, чем к переданной или даже перейдет в другую разрешенную комбинацию. В соответствии с этим, условие исправления всех ошибок кратностью не более $g_и$ можно записать

$$g_и \le \frac{d_{min} - 1}{2}. \qquad (22)$$

Из (19) и (21) следует, что если код исправляет все ошибки кратностью $g_и$, то число ошибок, которые он может обнаружить, равно $g_0 = 2 \cdot g_и$. Следует отметить, что соотношения (19) и (21) устанавливают лишь гарантированное минимальное число обнаруживаемых или

исправляемых ошибок при заданном d_{min} и не ограничивают возможность обнаружения ошибок большей кратности. Например, простейший код с проверкой на четность с d_{min}=2 позволяет обнаруживать не только одиночные ошибки, но и любое нечетное число ошибок в пределах $g_0<n$.

Корректирующие возможности кодов. Вопрос о минимально необходимой избыточности, при которой код обладает нужными корректирующими свойствами, является одним из важнейших в теории кодирования. Этот вопрос до сих пор не получил полного решения. В настоящее время получен лишь ряд верхних и нижних оценок (границ), которые устанавливают связь между максимально возможным минимальным расстоянием корректирующего кода и его избыточностью.

Так, граница Плоткина дает верхнюю границу кодового расстояния d_{min} при заданном числе разрядов n в кодовой комбинации и числе информационных разрядов k, и для двоичных кодов:

$$d_{\min} \le \frac{n \cdot 2^{k-1}}{2^k - 1} \qquad (23)$$

или

$$r \ge 2 \cdot (d_{\min} - 1) - \log_2 d_{\min} \qquad (24)$$

при $n \ge 2 \cdot n \cdot d_{\min} - 1$.

Верхняя граница Хемминга устанавливает максимально возможное число разрешенных кодовых комбинаций (2^k) любого помехоустойчивого кода при заданных значениях n и d_{min}:

$$2^k \le \frac{2^n}{\sum_{i=0}^{\frac{d_{\min}-1}{2}} C_n^i}, \qquad (25)$$

где C_n^i – число сочетаний из n элементов по i элементам.

Отсюда можно получить выражение для оценки числа проверочных символов

$$r \ge \log_2 \left(\sum_{i=0}^{\frac{d_{\min}-1}{2}} C_n^i \right). \qquad (26)$$

Для значений $(d_{min}/n) \le 0{,}3$ разница между границей Хемминга и границей Плоткина сравнительно невелика.

Граница Варшамова–Гильберта для больших значений n определяет нижнюю границу для числа проверочных разрядов, необходимого для обеспечения заданного кодового расстояния:

$$r \geq \log_2\left(\sum_{i=0}^{d-2} C_{n-1}^{i}\right). \qquad (27)$$

Отметим, что для некоторых частных случаев Хемминг получил простые соотношения, позволяющие определить необходимое число проверочных символов:

$$r \geq \log_2(n+1) \text{ для } d_{min}=3,$$
$$r \geq \log_2(2 \cdot n) \text{ для } d_{min}=4.$$

Блочные коды с $d_{min}=3$ и 4 в литературе обычно называют кодами Хемминга.

Все приведенные выше оценки дают представление о верхней границе числа d_{min} при фиксированных значениях n и k или оценку снизу числа проверочных символов r при заданных k и d_{min}.

Существующие методы построения избыточных кодов решают в основном задачу нахождения такого алгоритма кодирования и декодирования, который позволял бы наиболее просто построить и реализовать код с заданным значением d_{min}. Поэтому различные корректирующие коды при одинаковых d_{min} сравниваются по сложности кодирующего и декодирующего устройств. Этот критерий является в ряде случаев определяющим при выборе того или иного кода.

4.6 Корректирующие коды Хемминга

Построение кодов Хемминга базируется на принципе проверки на четность веса W (числа единичных символов) в информационной группе кодового блока.

Поясним идею проверки на четность на примере простейшего корректирующего кода, который так и называется кодом с проверкой на четность или кодом с проверкой по паритету (равенству).

В таком коде к кодовым комбинациям безызбыточного первичного двоичного k-разрядного кода добавляется один дополнительный разряд (символ проверки на четность, называемый проверочным, или контрольным). Если число символов 1 исходной кодовой комбинации четное, то в дополнительном разряде формируют контрольный символ 0, а если число символов 1 нечетное, то в дополнительном разряде формируют символ 1. В результате общее число символов 1 в любой передаваемой кодовой комбинации всегда будет четным.

Таким образом, правило формирования проверочного символа сводится к следующему:

$$r_1 = i_1 \oplus i_2 \oplus \ldots \oplus i_k,$$

где i – соответствующий информационный символ (0 или 1); k – общее их число а под операцией "$\oplus$" здесь и далее понимается сложение по mod 2. Очевидно, что добавление дополнительного разряда увеличивает общее число возможных комбинаций вдвое по сравнению с числом комбинаций исходного первичного кода, а условие четности разделяет все комбинации на разрешенные и неразрешенные. Код с проверкой на четность позволяет обнаруживать одиночную ошибку при приеме кодовой комбинации, так как такая ошибка нарушает условие четности, переводя разрешенную комбинацию в запрещенную.

Критерием правильности принятой комбинации является равенство нулю результата S суммирования по mod 2 всех n символов кода, включая проверочный символ r_1. При наличии одиночной ошибки S принимает значение 1:

$$S = r_1 \oplus i_1 \oplus i_2 \oplus \ldots \oplus i_k = \begin{cases} 0- \text{ ошибки нет,} \\ 1- \text{ однократная ошибка} \end{cases}$$

Этот код является (k+1, k)-кодом, или (n, n–1)-кодом. Минимально расстояние кода равно двум (d_{min}=2), и, следовательно, никакие ошибки не могут быть исправлены. Простой код с проверкой на четность может использоваться только для обнаружения (но не исправления) однократных ошибок.

Увеличивая число дополнительных проверочных разрядов и формируя по определенным правилам проверочные символы r, равные 0 или 1, можно усилить корректирующие свойства кода так, чтобы он позволял не только обнаруживать, но и исправлять ошибки. На этом и основано построение кодов Хемминга.

Коды Хемминга позволяют исправлять одиночную ошибку, с помощью непосредственного описания. Для каждого числа проверочных символов r=3, 4, 5… существует классический код Хемминга с маркировкой

$$(n, k)=(2^r-1, 2^r-1-r), \qquad (28)$$

т.е. (7,4), (15,11), (31,26) …

При других значениях числа информационных символов k получаются так называемые усеченные (укороченные) коды Хемминга.

Так, для Международного телеграфного кода МТК-2 , имеющего 5 информационных символов, потребуется использование корректирующего кода (9,5), являющегося усеченным от классического кода Хемминга (15,11), так как число символов в этом коде уменьшается (укорачивается) на 6. Для примера рассмотрим классический код Хемминга (7,4), который

можно сформировать и описать с помощью кодера, представленного на рис. 1. В простейшем варианте при заданных четырех (k=4) информационных символах (i_1, i_2, i_3, i_4) будем полагать, что они сгруппированы в начале кодового слова, хотя это и не обязательно. Дополним эти информационные символы тремя проверочными символами (r=3), задавая их следующими равенствами проверки на четность, которые определяются соответствующими алгоритмами:

$$r_1 = i_1 \oplus i_2 \oplus i_3;$$
$$r_2 = i_2 \oplus i_3 \oplus i_4;$$
$$r_3 = i_1 \oplus i_2 \oplus i_4.$$

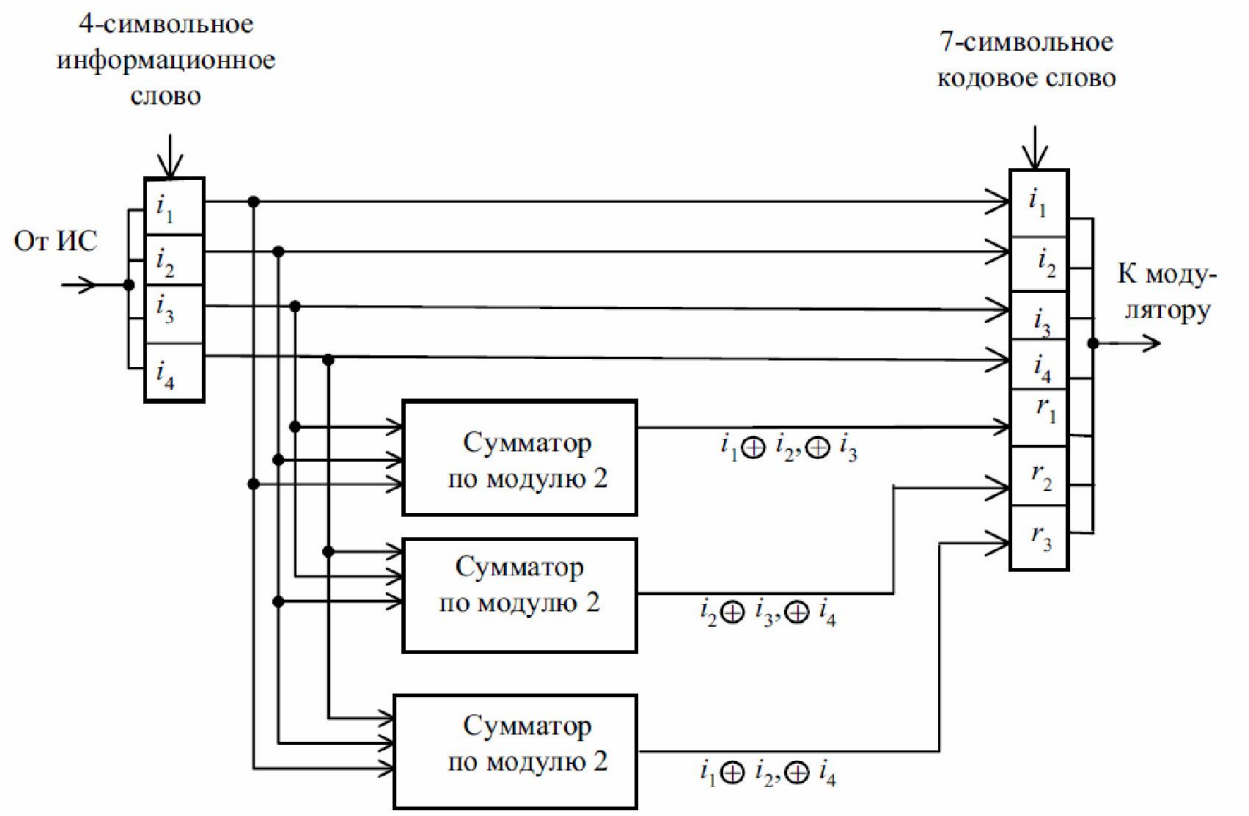

Рис. 1

На рис. 3.3 приведена схема декодера для (7,4) – кода Хемминга, на вход которого поступает кодовое слово V= (i_1', i_2', i_3', i_4', r_1', r_2', r_3'). Апостроф означает, что любой символ слова может быть искажен помехой в канале передачи.

В декодере в режиме исправления ошибок строится последовательность:

$$s_1 = r_1' \oplus i_1' \oplus i_2' \oplus i_3';$$
$$s_2 = r_2' \oplus i_2' \oplus i_3' \oplus i_4';$$
$$s_3 = r_3' \oplus i_1' \oplus i_2' \oplus i_4'.$$

Трехсимвольная последовательность (s_1, s_2, s_3) называется *синдромом*. Синдром $S=(s_1, s_2, s_3)$ представляет собой сочетание результатов проверки на четность соответствующих символов кодовой группы и характеризует определенную конфигурацию ошибок (шумовой вектор).

Число возможных синдромов определяется выражением

$$S=2^r. \qquad (29)$$

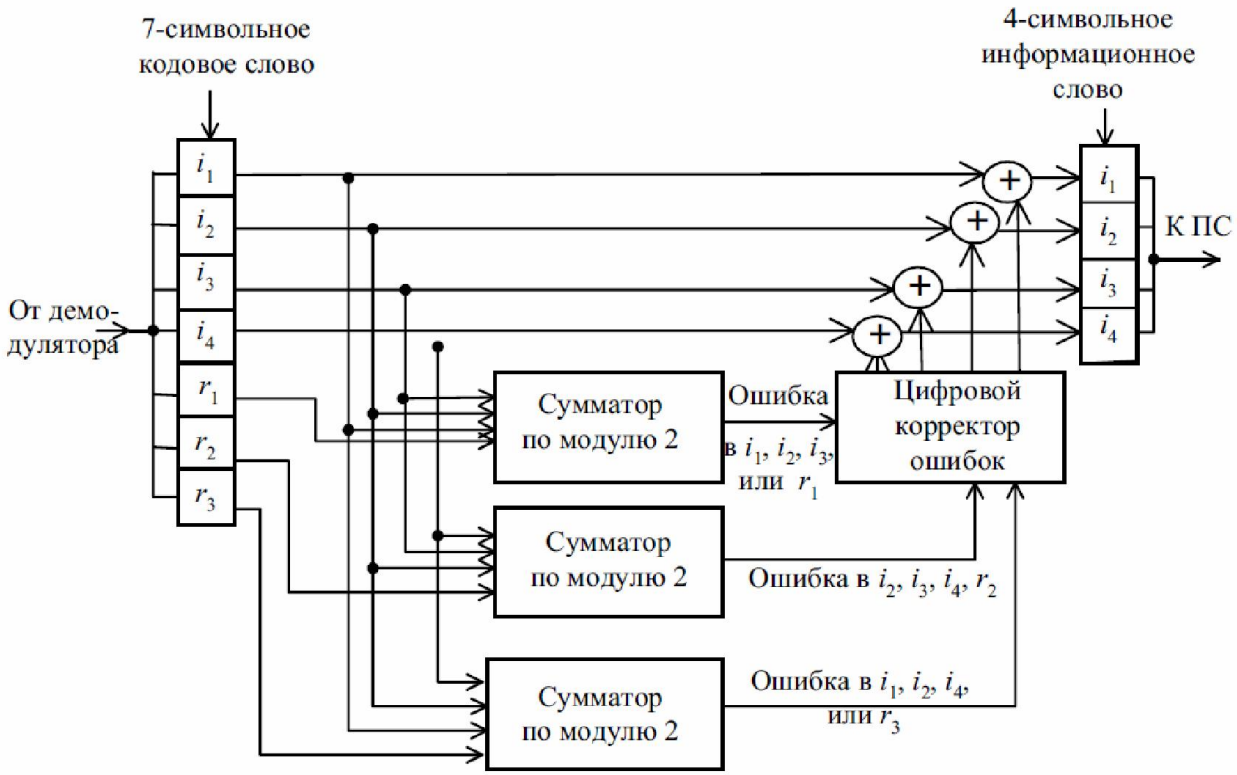

Рис. 2

При числе проверочных символов $r=3$ имеется восемь возможных синдромов ($2^3=8$). Нулевой синдром (000) указывает на то, что ошибки при приеме отсутствуют или не обнаружены. Всякому ненулевому синдрому соответствует определенная конфигурация ошибок, которая и исправляется. Классические коды Хемминга (28) имеют число синдромов, точно равное их необходимому числу (что позволяет исправить все однократные ошибки в любом информативном и проверочном символах) и

включают один нулевой синдром. Такие коды называются *плотноупакованными*.

Усеченные коды являются *неплотноупакованными*, так как число синдромов у них превышает необходимое. Так, в коде (9,5) при четырех проверочных символах число синдромов будет равно 2^4=16, в то время как необходимо всего 10. Лишние 6 синдромов свидетельствуют о неполной упаковке кода (9,5).

Для рассматриваемого кода (7,4) в табл. 1 представлены ненулевые синдромы и соответствующие конфигурации ошибок.

Табл. 1

Синдром	001	010	011	100	101	110	111
Конфигурация ошибок	00000001	0000010	0001000	0000100	1000000	0010000	0100000
Ошибка в символе	r_3	r_2	i_4	r_1	i_1	i_3	i_2

Таким образом, код (7,4) позволяет исправить все одиночные ошибки. Простая проверка показывает, что каждая из ошибок имеет свой единственный синдром. При этом возможно создание такого цифрового корректора ошибок (дешифратора синдрома), который по соответствующему синдрому исправляет соответствующий символ в принятой кодовой группе. После внесения исправления проверочные символы r_i можно на выход декодера (рис. 2) не выводить. Две или более ошибок превышают возможности корректирующего кода Хемминга, и декодер будет ошибаться. Это означает, что он будет вносить неправильные исправления и выдавать искаженные информационные символы.

Идея построения подобного корректирующего кода, естественно, не меняется при перестановке позиций символов в кодовых словах. Все такие варианты также называются (7,4)-кодами Хемминга.

Контрольные вопросы и задания

1. Какие коды называются равнодоступными?
2. В чем заключается сущность помехоустойчивого кодирования?
3. Какие задачи решают помехоустойчивые коды?
4. Какой код называется кодом с проверкой по паритету?
5. В чем заключается сложность выбора корректирующего кода для реальных каналов связи?
6. Какие коды называются блочными?
7. . Какие коды называются непрерывными?

8. Приведите примеры равномерных и неравномерных кодов.
9. Какова особенность неразделимых кодов? Приведите пример неразделимого кода.
10. Какие коды называются систематическими? Каковы их основные свойства?
11. Перечислите основные классы систематических кодов.
12. Перечислите основные характеристики корректирующих кодов.
13. Что такое минимальное кодовое расстояние?
14. Укажите количественную связь между минимальным кодовым расстоянием и корректирующей способностью кода.
15. Что определяет верхние границы для кодового расстояния?
16. Что определяет нижние границы для кодового расстояния?
17. Определите границы Плоткина и Хемминга для кодов (6,3) и (7,4), имеющих dmin = 3.
18. Определите границу Варшамова–Гильберта для этих же кодов.
19. Дайте определение синдрома ошибок.
20. Закодируйте целые числа от 5 до 8 кодом Хемминга (7,4), пользуясь уравнениями для проверок.
21. Дайте определение шумового вектора.
22. Определите шумовой вектор для конфигурации из одной ошибки в пятой позиции кода (9,5).
23. Определите шумовой вектор для конфигурации из двух ошибок в пятой и седьмой позициях кода (9,5).
24. Чему равны скорость и избыточность кода (9,5)?
25. Сколько всего синдромов ошибок может содержать таблица декодирования кода (9,5)?

Содержание