Нормативное обеспечение информационной безопасности. Лекции

Максим Захаров

Содержание

1. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТЕЙ ЭЛЕКТРОСВЯЗИ

1.1. Обеспечение безопасности сетей электросвязи

1.1.1. Общие положения и терминология

Основными функциями сетей электросвязи (СЭС), которые являются составными компонентами сети связи общего пользования единой сети электросвязи России, являются приём, обработка, хранение, передача и предоставление требуемой информации пользователям и органам государственного управления для её последующего применения.

СЭС предназначены для оказания услуг связи любому пользователю путём предоставления открытых информационных ресурсов и информации, не содержащей ССГТ или информации, доступ к которой ограничен в соответствии с законодательством РФ.

Под безопасностью СЭС понимается её способность противодействовать определённому 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 СЭС понимается совокупность информационных ресурсов и инфраструктуры СЭС.

Инфраструктура СЭС определяется как совокупность средств связи, линий связи, сооружений связи, технологических систем связи, технологий и организационных структур, обеспечивающих информационное взаимодействие компонентов СЭС.

Информационные ресурсы СЭС — это совокупность хранимых (используемых для обеспечения функционирования процессов СЭС), обрабатываемых и передаваемых данных, содержащих информацию пользователей и/или системы управления СЭС.

Под устойчивостью функционирования СЭС понимается способность СЭС 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 СЭС является взаимоувязанная совокупность организационных, аппаратных, программных и программно-аппаратных средств, способов, методов, правил и процедур, используемых для реализаций требований к безопасности СЭС.

Нарушитель безопасности СЭС — физическое или юридическое лицо, преступная группа, процесс или событие, производящее 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 СЭС понимается вероятность причинения ущерба СЭС или её компонентам вследствие того, что определённая угроза реализуется в результате наличия определённой уязвимости в СЭС.

Угрозой безопасности СЭС является совокупность условий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба СЭС или её компонентам.

Уязвимость СЭС определяется как недостаток или слабое место в средстве связи, техническом процессе (протоколе) обработки/передачи информации, мероприятиях и механизмах обеспечения безопасности СЭС, позволяющие нарушителю совершать действия, приводящие к успешной реализации угроз безопасности.

Система обеспечения безопасности системы связи общего пользования — совокупность служб безопасности операторов средств ССОБ и используемых ими механизмов обеспечения безопасности, взаимодействующая с органами управления СЭС, организация и функционирование которой осуществляется по нормам правилами и обязательным требованиям, установленных в области связи.

Под службой безопасности СЭС понимается организационная техническая структура оператора СЭС, реализующая политику безопасности оператора связи и обеспечивающая функционирование системы обеспечения безопасности СОБ.

Политикой безопасности оператора связи является совокупность документированных правил, процедур, практических приёмов и 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 приём знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме проводной, оптической или другим электромагнитным системам.

1.1.2. СЭС, их информационны ресурсы и проблемы обеспечения безопасности

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

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

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

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

Необходимость рассмотрения проблем обеспечения безопасности сетей электросвязи обусловлена:

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

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

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

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

1.1.3. Основными целями обеспечения безопасности СЭС

Основными целями обеспечения безопасности сетей электросвязи являются:

- достижение устойчивого функционирования и успешного выполнения заданных функций сетью электросвязи, в условиях возможного ВН, способного привести к нарушению конфиденциальности, целостности, доступности или подотчетности;
- обеспечение доступности услуг связи, особенно услуг экстренного обслуживания в чрезвычайных

ситуациях, в том числе и в случае террористических актов.

Основными задачами обеспечения безопасности сетей электросвязи являются:

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

- предотвращение, обнаружение угроз безопасности, пресечение их реализации и своевременная ликвидация последствий возможных ВН, в том числе и террористических действий;
- организация системы пропуска приоритетного трафика по сети электросвязи в случае чрезвычайных ситуаций, организация бесперебойной работы международной аварийной службы;
- совершенствование и стандартизация применяемых мер обеспечения безопасности сетей электросвязи.

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

Оператор связи при осуществлении процесса управления функционированием сети электросвязи должен минимизировать возможные негативные ВН для обеспечения выполнения основных целей организации связи, в том числе и бизнес-процессов. Это достигается путем интегрирования в систему управления функционированием сети электросвязи процесса управления рисками. На каждой стадии жизненного цикла сетей электросвязи (проектирование, строительство, реконструкция, развитие и эксплуатация) должна осуществляться деятельность по поддержанию управления рисками, основой которой являются процессы идентификации и оценки рисков.

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

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

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

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

1.1.4. Угрозы безопасности СЭС. Модели угроз.

Источником угроз безопасности СЭС могут быть:

1. Субъект.
2. Материальный объект.
3. Физическое явление.

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

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

обработки, передачи, хранения информации подвержены большому количеству 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:

1. Уничтожение информации и/или других ресурсов.
2. Искажение или модификация информации.
3. Мошенничество.
4. Кража, утечка, потеря информации или других ресурсов.
5. Несанкционированный доступ.
6. Отказ в обслуживании.

Каждая выявленная угроза в соответствии с выбранной методикой оценкой риска должна ранжироваться по вероятности своего возникновения для последующего анализа рисков и оценки величины возможного ущерба СЭС от реализации угроз.

Пример трёхуровневой градации вероятности возникновения угроз.

Описание показателей вероятности возникновения угроз.

Показатель вероятности	Описание действий нарушителя
Маловероятный	Нарушитель обладает очень незначительными техническими возможностями для реализации угрозы или мотивация для нарушителя очень низкая.
Вероятна	Технические возможности, необходимые для реализации угрозы не слишком высоки и разрешимы без большого усилия, кроме того должно быть разумное для нарушителя побуждения, чтобы реализовать угрозу.
Возможна	На СЭС отсутствуют механизмы обеспечения безопасности, используемые для противодействия этой угрозе и побуждение для нарушителя весьма высока.

В целях учёта 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 безопасности к сети и разработчик, создающий эту сеть и службы обеспечения ИБ сети при её эксплуатации.

Модель угроз должна включать:

1. Описание ресурсов инфокоммуникационной структуры (объектов безопасности) СЭС, требующих защиты.
2. Описание источников формирования дестабилизирующих воздействий и их потенициальных возможностей.

3. Стадии жизни цикла СЭС, в т. ч. определяющий её технологический и эксплуатационный этапы.
4. Описание процесса возникновения угроз и путей их практической реализации.

К 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 возможная мера обеспечения безопасности для противодействия каждой конкретной угрозе.

1.2. Нарушители безопасности СЭС

1.2.1. 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 её 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.

Нарушителя безопасности СЭС могут быть:

1. Террористы и террористические организации.
2. Конкурирующие организации и структуры.
3. Спецслужбы иностранных государств и блоков государств.
4. Криминальные структуры.
5. Взломщики программных продуктов ИТ, использующихся с системах связи.
6. Бывшие сотрудники организации связи.
7. Недобросовестные сотрудники и партнёры.
8. Пользователя услугами связи и др.

Основными мотивами нарушений безопасности СЭС могут быть:

1. Месть.
2. Достижение денежной выгоды.
3. Хулиганство и любопытство.
4. Профессиональное самоутверждение.

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

Задача построения модели нарушителя безопасности СЭС состоит в определении:

1. Штатных объектов или элементов сети, к которым возможен доступ.
2. Субъектов, допущенных к работе с оборудованием сети в период её проектирования, разработки, развёртывания и эксплуатации.
3. Перечня соответствия объета доступа к субъекта, которые могут быть потенциальными нарушителями.

При определении потенциального нарушителя и составления 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.

1.2.2. Направленность и характер воздействий нарушителя безопасности СЭС

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

Воздействия нарушителя могут осуществляться:

1. По каналам абонентского доступа, в т. ч. и беспроводным.
2. По внутренним линиям связи.
3. С рабочих мест систем управления и технического обслуживания.
4. По недекларированным каналам доступа.

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

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

Непреднамеренные случайные воздействия могут быть спровоцированы:

1. Недостаточной надёжностью средств связи.
2. Ошибками обслуживающего персонала.
3. Природными явлениями.
4. Другими объективными дестабилизирующими факторами.

Преднамеренные воздействия могут быть:

1. Активными.
2. Пассивными.
3. Не преследующими цели.

Активные действия нарушителя предусматривают вмешательство в работу СЭС, нарушение режимов её функционирования и снижение качества обслуживания вплоть до полного прекращения предоставления услуг связи пользователям.

Основные цели активных действий:

1. Подрыв репутации оператора-конкурента путём нарушения доступности услуг связи и (или) ухудшения её характеристик.
2. Несанкционированное использование услуг.

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

1. Перехват персональных данных пользователей (например паролей для регистрации терминалов).
2. Перехват данных о финансовых сделках с целью нанесения ущерба бизнесу.
3. Наблюдение за выполняемым процессом (подготовка для новых атак, активных действий).
4. Поиск идеологических, политических выгод.
5. Шантаж, вымогательство.

Действия, непреследующие цели (хулиганство) — действия, не ставящие цели нанесения вреда конкретному физическому объекту или лицу.

1.3. Критерии безопасности СЭС. Последствия нарушений безопасности СЭС.

Критерии безопасности СЭС:

1. Конфиденциальность инфокоммуникационной структуры СЭС.
2. Целостностью информации услуг связи.
3. Доступностью информации услуг связи.
4. Подотчётностью действий в сети.

Под конфиденциальностью инфокоммуникационной структуры СЭС понимают свойства, позволяющие ограничить НСД к инфокоммуникационной структуре СЭС и (или) не раскрывать содержания инфокоммуникационной

лицам, объектам или процессам. Нарушение конфиденциальности — несанкционированное раскрытие информации управления персональных данных пользователей

Под целостностью информации 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 т. ч. в чрезвычайных ситуациях.

Нарушение целостности — несанкционированная модификация разрушение информационных ресурсов и структуры СЭС.

Под доступностью информации услуг понимается способность СЭС обеспечить пользователям согласованные условия доступа к предоставляемым услугам связи и их получение в т. ч. в условиях возможных воздействиях нарушителя на инфокоммуникационную структуру СЭС.

Нарушение доступность — нарушение доступа к пользованию информацией и услуг связи.

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

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

В таблице показана взаимосвязь основных угроз и критериев безопасности СЭС.

Вид угрозы	К	Ц	Д
Уничтожение информации и (или) др. ресурсов	-	+	+
Искажение или модификация информации	-	+	-
Мошенничество	+	+	+
Кража, утечка, потеря утечка информации	+	+	+
НСД	+	+	+
Отказ в обслуживании	-	+	+

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

1. Низкое потенциальное воздействие может привести к ограниченному неблагоприятному эффекту.
2. Умеренное потенциальное воздействие может привести к серьёзному неблагоприятному эффекту.
3. Высокое потенциальное воздействие может привести к тяжёлому или катастрофическому неблагоприятному эффекту.

В соответствии с используемой оператором связи методикой оценки рисков и с учётом вероятностей возникновения угрозы и потенциального воздействия нарушителя по реализации данной угрозы должен определяться риск возможного нанесения ущерба СЭС.

Величина риска может классифицироваться 3 показателями, приведёнными в таблице. Описание показателей величины возможного риска.

Уровень значения показателя величина риска	Описание риска
Незначительный	Незначительные риски возникают, если атаки нарушителя являются маловероятными. Угрозы, причиняющие незначительные риски, считаются допустимыми
Существенные	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

1.4. Принципы обеспечения безопасности СЭС в условиях воздействия нарушителя

Обеспечение безопасности должно осуществляться с учётом основных принципов:

1. Комплексности использования всей совокупности нормативно-правовых актов, организационных и режимных мер, программных, аппаратных и программно-аппаратных методов защиты, обеспечивающих безопасное функционирование СЭС.
2. Защищённости сбалансированных интересов пользователей, операторов связи и органов государственного управления.
3. Управляемости методами, действиями и процедурами по обеспечению безопасности сетей электросвязи и контролю качества процессов передачи информации в условиях возможных ВН на инфокоммуникационную структуру сетей в соответствии с функциями системы управления сетью.
4. Непрерывности совершенствования методов, действий и процедур по обеспечению безопасности сетей электросвязи с учетом достигнутого

отечественного и зарубежного опыта в условиях возможных ВН и изменения методов и средств этих воздействий.

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

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

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

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

1.5. Общие требования к безопасности СЭС

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

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

Требования по обеспечению безопасности конкретной сети электросвязи должны формироваться с учетом:

- целей, функций и задач решаемых оператором связи,
- условий использования сети электросвязи в общей системе связи государства,
- специфики используемой технологии передачи информации,
- потенциальных угроз безопасности и возможных воздействий нарушителя,
- реальных проектных и эксплуатационных ресурсов и существующих ограничений на функционирование сети электросвязи,
- требований и условий взаимодействия с другими сетями электросвязи.

Предоставление и использование услуг и механизмов обеспечения безопасности может быть довольно дорогим относительно потерь при нарушении безопасности сетей электросвязи. Поэтому должно анализироваться

соотношение между стоимостью мер по обеспечению безопасности и возможными финансовыми последствиями нарушения безопасности, при этом важно определить конкретные требования к безопасности в соответствии с услугами, подлежащими защите.

Требования по обеспечению безопасности сетей электросвязи включают:

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

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

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

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

1.6. Основные мероприятия по обеспечению безопасности СЭС

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

Мероприятия по обеспечению безопасности сети электросвязи, проводимые оператором связи, не должны ухудшать качественных характеристик сети и снижать оперативность обработки информации. Реализация обязательных требований к безопасности, установленных федеральными органами исполнительной власти в области связи, осуществляется силами и средствами владельца сети электросвязи с привлечением при необходимости специализированных организаций, имеющих лицензии на данный вид деятельности.

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

Вопросы непосредственного обеспечения безопасности при присоединении одной сети электросвязи к другой и условия выполнения обязательных

требований к безопасности, установленные федеральными органами исполнительной власти в области связи, при взаимодействии этих сетей оговариваются в заключаемых операторами связи договорах о присоединении сетей электросвязи.

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

Обеспечение безопасности сетей электросвязи достигается:

1. защитой сетей электросвязи от НСД к ним и передаваемой посредством их информации;
2. противодействием техническим разведкам;
3. противодействием сетевым атакам и вирусам;
4. защитой средств связи и сооружений связи от НСВ, включая физическую защиту сооружений и линий связи;
5. разграничением доступа пользователей и субъектов инфокоммуникационной структуры сетей электросвязи к информационным ресурсам в соответствии с принятой политикой безопасности оператора связи;
6. использованием механизмов обеспечения безопасности;
7. физической и инженерно-технической защитой объектов инфокоммуникационной структуры сетей электросвязи;
8. использованием организационных методов, включающих:

    - разработку и реализацию политики безопасности оператором связи;
    - организацию контроля состояния безопасности сети электросвязи;
    - определение порядка действий в чрезвычайных ситуациях и в условиях чрезвычайного положения;
    - определения порядка реагирования на инциденты безопасности;
    - разработку программ повышения информированности персонала сети электросвязи в вопросах понимания им проблем безопасности;
    - определение системы подготовки и повышения квалификации специалистов в области безопасности.

Пользователи услугами связи имеют право применять специальные механизмы обеспечения безопасности и СЗИ, разрешённые к применению на СЭС и сертифицированные в соответствии с действующим законодательством РФ.

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

- только авторизованные пользователи должны иметь доступ к сетям электросвязи и использованию предоставляемых им услуг;
- авторизованные пользователи должны иметь доступ и оперировать только теми ресурсами, к которым они допущены;
- все пользователи должны быть ответственными за их собственные, и только их собственные, действия в сети электросвязи.

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.

1.7. Основные положения о структуре системы обеспечения безопасности сетей электросвязи

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

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

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

1. уровень управления безопасностью. На данном уровне осуществляется управление безопасностью сетей электросвязи, координируемое центральным органом СОБ;
2. организационно-административный уровень. Включает службы (отделы, подразделения, администраторов) безопасности, в зависимости от структуры организации связи. На данном уровне осуществляются:

    - взаимодействие с системой управления сетями электросвязи;
    - управление, координация и контроль проводимых организационных и технических мероприятий на всех нижележащих уровнях;
    - учет практического применения нормативной правовой базы (законов, стандартов, положений, должностных инструкций, планов по безопасности);

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

    - разграничение доступа к информационным ресурсам, сетевым объектам и системе управления сетью электросвязи,
    - защита от НСД, аутентификация и идентификация участников сетевого взаимодействия, включая удаленные объекты и администраторов (сетевых и безопасности),
    - контроль трафика (межсетевые экраны), средства обнаружения атак, средства регистрации и учета событий и ресурсов (аудит и мониторинг безопасности);

4. уровень безопасности услуг. На данном уровне осуществляется контроль качества обслуживания (предоставляемых услуг связи) в условиях возможных ВН и в чрезвычайных ситуациях, в том числе целостности циркулирующих в сети сообщений, содержащих данные пользователя и информацию управления;
5. уровень сетевой безопасности. Данный уровень поддерживает безопасность сетевых протоколов, которые обеспечивают:

    - передачи трафика из конца в конец,
    - транспортирование файлов,
    - поддержку фундаментальных приложений, передачу голоса в сети и электронную почту;
    - конфиденциальность передаваемой по каналам связи информации управления;

6. уровень физической безопасности. На данном уровне обеспечиваются:

- физическая охрана помещений, в которых обрабатывается и хранится информация,
- организация контроля доступа сотрудников и посетителей на территорию организации связи, в помещения со средствами связи, осуществляющими обработку информации, к технологическим системам управления, кабельным соединениям,
- организация охранной сигнализации,
- контроль вскрытия аппаратуры,
- 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 сети электросвязи должна предусматривать формирование организационно-штатной структуры (отдел, подразделение, администратор безопасности) для непосредственного проведения мероприятий безопасности сети электросвязи.

2. Домашняя работа

2.1. Модель угроз безопасности для корпоративной сети связи ВУЗА

2.1.1. Ресурсы инфокоммуникационной структуры СЭС, требующие защиты:

1. Абонентская база данных в памяти коммутатора.
2. Программное обеспечение АТС.
3. Аппаратная часть АТС.
4. Абонентская сеть связи.

2.1.2. Источники формирования дестабилизирующих воздействий и их потенициальные возможности:

1. **Производитель АТС**. Является специалистом высшей квалификации, знает все возможности АТС и, в частности, о системе и средствах ее защиты и скрытых возможностях. Не имеет физического доступа в КЗ, но может осуществить удалённый доступ по недекларированному каналу к АТС.
2. **Террорист**. Не является абонентов сети, не обладает знаниями о функционировании АС.
3. **Сотрудник университета**. Имеет общие представления о функционировании сети связи, имеет доступ к штатным средствам сети связи (может совершать звонки).

4. **Сотрудник университета, обслуживающий АТС**. Является специалистом высшей квалификации, знает все об АТС и, в частности, о системе и средствах ее защиты. Имеет доступ в контролируемую зону — к аппаратной части АТС. Имеет доступ к утилитам администрирования и конфигурирования системы.

2.1.3. Описание возникновения угрозы:

1. Производитель заложил в АТС незадокументированную возможность удалённого доступа, которая позволяет дистанционно отлаживать неисправную систему в тех условиях, в которых она неисправно работает. Она также дает возможность дистанционно обновлять системы с обнаруженными дефектами. Это наиболее опасная уязвимость, т.к. доступ злоумышленника к программному обеспечению дает практически неограниченный доступ к АТС и сети.
2. Сотрудник университета, обслуживающий АТС, узнаёт о своём сокращении и решает отомстить руководству Университета. Он использует штатную утилиту проверки/модификации станционной базы данных: такая утилита позволяет исследовать и модифицировать базу данных системы для устранения неисправностей из-за неправильной конфигурации, ошибки конструкции и т.п. Он меняет маршрутизацию в сети. В результате работа сети нарушена.
3. Террорист с целью самоутверждения, придания своей деятельности особой значимости проникает через проходную Университета и закладывает бомбу рядом с комнатой, где расположена АТС. Реализована атака типа отказ в обслуживании.
4. Сотрудник университета в корыстных целях подключает устройство записи к абонентской линии ректора Университета и ведёт прослушивание конфиденциальных переговоров с целью перепродажи данных сведений заинтересованным лицам.

2.1.4. Стадии жизни цикла СЭС:

1. Предпроектный анализ.
2. Проектирование системы.
3. Разработку системы.
4. Интеграцию и сборку системы, проведение ее испытаний.
5. Эксплуатацию системы и ее сопровождение.
6. Развитие системы.

3. ГОСТ 15408

3.1. Основные понятия, общие критерии (ОК)

ОК содержат 2 основных требования вида безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим им механизмам;
- требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

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

Безопасность в ОК рассматривается на жизненном цикле ОО.

Кроме того, объект оценки рассматривается в контексте среды безопасности, характеризующейся определёнными условиями и угрозами. Требования в общих критериях формулируются в документах 2 видов:

- профиля защиты (ПЗ). Типовой набор требования, которым должны удовлетворять продукты и (или) системы определённого класса;
- задания по безопасности (ЗБ). Содержит совокупность требований к конкретной разработке продукта или системы.

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

Продукт ИТ представляет собой совокупность средств ИТ, предоставляющих определённые функциональные возможности и предназначенных для непосредственного использования либо включения в различные системы. Продукт или система могут быть уже существующими или проектируемыми.

В среду безопасности объекта оценки включаются:

1. Законодательная среда (нормативные акты, затрагивающие объекты оценки).
2. Административная среда (положения политик и программ безопасности, учитывающие особенности объекта оценки).
3. Процедурная среда (физическая среда объекта оценки и меры и его физической защиты, персонал и его свойства, принятые эксплуатационные и иные процедуры).
4. Программно-техническая среда (предназначение объекта оценки и предполагаемая область его применения, активы (ресурсы, которые требуют защиты объектами оценки)).

Из анализа среды безопасности должны быть описаны следующие объекты:

1. Предположение безопасности, которое выделяет объект оценки из общего контекста, задаёт границы рассмотрения. Истинность этих предположений принимается без доказательств, а из множества возможных отбираются только те, что заведомо необходимы для обеспечения безопасности объект оценки.
2. Угрозы безопасности объекту оценки, наличие которых в рассматриваемой среде установлено или предполагается. Они характеризуются следующими параметрами:

    - источник;
    - метод воздействия;
    - опасные с точки зрения закономерности использования уязвимости;
    - активы, потенциально подверженные повреждению. При анализе рисков угроз принимается во внимание вероятность активации угрозы и её 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 объекту оценки. Для системы ИТ такие положения могут быть описаны точно, для продукта ИТ в общих чертах.

На основании положений об учёте 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 объекта оценки и цели безопасности среды.

Общие критерии, а именно 2 и 3 части являются каталогами требований безопасности. В основу методологии общих критериев положена модель безопасности, представленная на рисунке.

Для структуризации пространства требований в ОК введения иерархия Класс - Семейство - Компонент - Элемент.

Классы определяют наиболее общую группировка требований. Семейства в пределах класса различаются по строгости и другим характерстикам. Компонент определяется минимальным набором требований, фигурирующим как единое целое. Элемент — это неделимое требование к безопасности.

Между критериями введены зависимости, когда компонент сам по себе недостаточен для достижения целей безопасности. После формулирования функциональных требования, требований доверия к объекту оценки и его среде в ПЗ и ЗБ можно приступать к оценке безопасности продукта или системы.

ПЗ от ЗБ отличается двумя разделами. В ЗБ добавляются краткая спецификация объекта оценки и утверждение о соответствии профилю защиты.

Профиль защиты включает в себя следующие разделы:

1. Введение, состоящее из подразделов идентификации ПЗ и аннотации ПЗ.
2. Описание объекта оценки.
3. Среда безопасности объекта оценки, состоящий из подразделов предположения безопасности, угроз, политик безопасности организации.
4. Цели безопасности, состоящие из подразделов целей безопасности для объекта оценки и целей безопасности для среды.
5. Требования безопасности ИТ, состоящие из требований безопасности для объекта оценки, включая функциональные требования, требования доверия безопасности к объекта оценки и требования безопасности для среды ИТ.
6. Замечания по применению и обоснование, состоящее из подразделов логического обоснования требований безопасности и логического обоснования целей безопасности. В ЗБ дополнительно имеются следующие разделы:

    - краткая спецификация объекта оценки, состоящая из функций безопасности объекта оценки и спецификации мер доверия;
    - утверждение соответствии профилю защиты, в котором приводится ссылка на ПЗ, конкретизация ПЗ и дополнения ПЗ.

Раздел введения дополняется разделом соответствия ОК. В раздел обоснования добавляются подраздел логического обоснования, краткая спецификация объекта оценки и логического обоснования утверждения о соответствии ПЗ. Краткая спецификация определяет отражение требования на функции безопасности.

Общие критерии не предписывают общей методологии или дисциплины разработки модели 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 аппаратура и реализация в виде исполняемых файлов, программных продуктов и т. п.

Между уровнями представления должно демонстрироваться соответствие, т. е. все сущности более высоких уровней обязаны фигурировать и ниже. А внизу не должно быть место лишним сущностям, не обусловленным потребностями более высоких уровней.

При проведении оценки главными являются следующие вопросы:

1. Отвечают ли функции безопасности объекта оценки функциональным требованиям.
2. Конкретна ли реализация функции безопасности.

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

3.2. Классификация функциональных требований безопасности

Часть 2 общих критериев описывает 11 классов, 66 семейств, 35 компонентов ФТБ и содержат требования 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 определённых положений политики безопасности.

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

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

Классы ФТБ 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 играю инфраструктурную роль.

К первой группе можно отнести следующие классы:

1. FAU. Аудит безопасности.
2. FIA. Идентификация и аутентификация.
3. 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 идентификация пользователей, аутентификации пользователей, определению атрибутов пользователя, связыванию пользователя с субъектом, к отказыванию от аутентификации и спецификации секретов.

Класс FRU включает 3 семейства, призванные разными способами поддерживать высокую доступность:

- отказоустойчивость,
- приоритет обслуживания,
- распределение ресурсов.

Ко 2 группе можно отнести следующие классы:

1. FCO. Связь.
2. FPR. Приватность.

Класс FCO состоит из 2 семейств неотказуемость отправки или получения данных, которая достигается путём 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:

- анонимности,
- псевдонимность,
- невозможность ассоциаций,
- скрытность.

Достичь высокоуровневых целей безопасности помогают 2 класса:

1. FDP. Защита данных пользователя.
2. FPT. Защита функций безопасности объекта оценки.

Класс FDP включает 13 семейств, которые можно разбить на 4 группы:

1. Политики защиты данных пользователя.
2. Виды защиты данных пользователя.
3. Импорт и экспорт данных пользователя.
4. Защита данных пользователя при передаче между доверенными продуктами и системами ИТ.

Класс FPT включает 16 семейств, которые можно условно разделить на 4 группы:

1. Архитектурная безопасность.
2. Защита реализаций функций безопасности.
3. Защита данных функций безопасности.
4. Инфраструктурные требования.

Наибольшее число компонентов сосредоточены в классах инфраструктурной группы.

1. FCS. Криптографическая поддержка.
2. FMT.
3. FTA. Доступ к объекту оценки.
4. FTP. Доверенный маршрут канала.

Класс FCS состоит из 2 семейств, где в самом общем виде рассматривается 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 методики отсутствуют.

Класс FMT, включает 16(?) семейств регулирует управление функциями безопасности и из данными атрибутами и ролями безопасности.

Класс FTA содержит 6 семейств, в которые вошли требования управления сеансами работы пользователей (помимо идентификации и аутентификации).

Класс FTP, состоящий из 2 семейств доверенный маршрут и доверенный канал, обеспечивает требования по созданию маршрутов/каналов передачи информации безопасным способом.

Пример описания функциональных требования. Рассмотрим описание класса, семейства, компонента элемента требований на примере класса FCO связь. Класс FCO содержит 2 семейства, связанные с уверенностью в идентичности сторон, участвующих в обмене данными. Идентичностью отправителя переданной информации (доказательства отправления) и идентичностью получателя переданной информации (доказательства получения). Эти семейства обеспечивают, что отправитель не сможет отрицать факт оправления сообщения, а получатель не сможет отрицать факт его получения. Декомпозиция класса на составляющие его компоненты показана на рисунке.

Семейство FCO_{NRO} обеспечивает невозможность отрицания отправителем информации факта её отправления. Семейство содержит требования, чтобы функции безопасности объекта оценки обеспечили метод предоставления субъекту получателю свидетельства оправления информации. Это свидетельство может быть верифицировано этим субъектом или другими субъектами.

Компоненты внутри семейства проранжированы иерархически последовательно. $FCO_{NRO}.1$ (избирательное доказательство отправления) содержит требования чтобы функции безопасности объекта оценки предоставили субъектам возможность запросить свидетельства отправления информации. $FCO_{NRO}.2$ (принудительное доказательство отправления) содержит требования, чтобы функции безопасности объекта оценки всегда генерировали свидетельства отправления передаваемой информации.

Управление: для функций управления для класса FMT может рассматриваться следующие действия.

- управление изменениями типов и полей информации, атрибутов отправителя информации и получателей свидетельств,
- аудит: $FCO_{NRO}.1$ — если в ПЗ или ЗБ включено семейство FAU_{GEN} генерация данных аудита безопасности, то следует предусмотреть возможность (в зависимости от выбранного уровня) аудита следующих действий/событий/параметров

  – минимальный: идентификатор пользователя, который запросил генерацию свидетельства отправления, обращение к функциям неот-

казуемости
  - базовый: идентификатор информации, получателя и копии предоставляемого свидедельства.
  - детализированный: идентификатор пользователя, который запросил верификацию свидетельства.

- аудит: $FCO_{NRO}.2$ — если в ПЗ или ЗБ включено семейство FAU_{GEN} генерация данных аудита безопасности, то следует предусмотреть возможность (в зависимости от выбранного уровня) аудита следующих действий/событий/параметров:

  - минимальный: обращение к функции неотказуемости.
  - базовый: идентификация информации, получателя и копии предоставляемого свидетельства.
  - детализированый: идентификатор пользователя, который запросил верификацию свидетельства.

Описание компонента $FCO_{NRO}.1$ избирательное доказательство отправления выглядит следующим образом:

- иерархический для $FCO_{NRO}.1$: нет подчинённых компонентов. Элементы компонента $FCO_{NRO}.1$ описаны ниже.

  - $FCO_{NRO}.1.1$ FBO функции безопасности объекта оценки должны быть способны генерировать свидетельство отправления передаваемой. [*Список типов информации*]. Передаваемой при забросе [выбор: отправитель-получатель,] [*назначение*: список третьих лиц]
  - $FCO_{NRO}.1.2$ FBO должны быть способны связать [назначение: список атрибутов] отправителя информации и [назначение: список информационных полей] информации, к которой прилагается свидетельство.
  - $FCO_{NRO}.1.3$ FBO должны предоставить возможность верифицировать свидетельство отправления информации [выбор: отправитель, получатель [назначение: список третьих лиц]] при установленных [назначение: ограничение на свидетельство отправления].

Зависимости данного компонента — $FIA_{UID}.1$ выбор момента идентификации.

3.3. Основные понятия, классификация требования доверия безопасности

Доверие в интерпретации ОК — это основа для уверенности в том, что продукт или система ИТ отвечает целям безопасности.

Доверие обеспечивается через активные исследование/оценку продукта или системы. Требования доверия безопасности (ТДБ) охватывают весь жизненный цикл объекта оценки и предполагают выполнение следующих действий:

1. Оцениваются ЗБ и ПЗ как источники требований безопасности.
2. Анализируются различные представления проекта объекта оценки и соответствия между ними, а также соответствия каждого из них требованиям безопасности.
3. Проверяются процессы и процедуры безопасности, их применение, анализируется документация, верифицируются представленные доказательства.
4. Анализируются тесты и их результаты, а также уязвимости объекта оценки.
5. Проводятся независимые тестирования, в т. ч. тестирование проникновения.

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

1. Элементы действий разработчика (помечаются буквой D после номера элемента). Эти действия должны подтверждаться доказательственным материалом (свидетельством).
2. Элементы представления и содержания свидетельств (помечаются буквой S).
3. 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 объекта оценки.

К первой группе, логически предшествующей разработке и оценке объекта оценки принадлежать классы:

1. APE оценка профиля защиты.
2. ASE оценка задания по безопасности.

Цель требований классов APE и ASE проверить полноту, непротиворечивость и реализуемость ПЗ или ЗБ.

Во вторую группу входят классы:

1. ADV разработка.
2. ALC поддержка жизненного цикла.

3. ACM управление конфигурацией.

Класс ADV состоит из 7 семейств и содержит требования для постепенного повышения уровня детализации проекта вплоть до предоставления реализаций с демонстрацией соответствия между уровнями. В этом классе предусмотрено 3 стиля изложения спецификации: неформальный, полуформальный и формальный — и 3 способа демонстрации соответствия.

Технологические требования процедурного характера составляют содержание класса ALC, состоящего из 4 семейств. Прежде всего определяется модель жизненного цикла (семейства ALC_{LCD}), затем следует обосновать выбор инструментальных средств и методов (семейства ALC_{TAB}). Безопасность разработки организуется в соответствии с требованиями семейства ALC_{DVC}. Важнейшим элементом этапа сопровождения является устранение недостатков (семейство ALC_{FLR}).

Управление конфигурацией ACM — необходимый инструмент коллектива разработчиков. В этот класс входит 3 семейства. Самый содержательный из них — ACM_{CAB}, специфицирующие возможности управления конфигурацией. Семейство ACM_{SCP} специфицирует область действий управления конфигурацией. Для уменьшения числа возможных ошибок управление конфигурацией следует максимально автоматизировать. В этом 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 2 семейств, где сформулированы требования к руководству администратора AGD_{ADM}, руководство пользователя AGD_{USR}.

Класс ATE состоит из 3 семейств, содержащих требования к полноте, глубине, способам и результатам тестирования функций безопасности на предмет из соответствия спецификациям.

Один из ключевых моментов оценки безопасности продуктов ИТ — оценка уязвимостей, отправным пунктом которой является анализ уязвимостей (семейства AVA_{VLA}), выполняемый разработчиком и оценщиком. Анализ стойкости функций безопасности объекта оценки (семейство AVA_{SOF}) проводится на уровне реализующих механизмов.

Требования семейство AVA_{MSV} (неправильное применение) направлены на то, чтобы исключить возможность такого конфигурирования и/или применения объекта оценки, которая 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 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 объекта оценки на соответствие общим критериям. 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 нём или в его среде. Речь идёт о выявлении новых угроз и уязвимостей, изменений в требованиях пользователей об исправлении ошибок.

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

Одна из целей общих критериев 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:

1. Расширение границ объекта оценки.
2. Увеличение уровня детализации рассматриваемых аспектов объекта оценки.
3. Повышение строгости рассмотрения и применение более формальных методов верификации.

3.4. Оценочный уровень доверия безопасности

В общих критериях определено 7 упорядоченных по возрастанию ОУД, содержащих рассчитанные на многократное применение комбинации требований доверия (не более 1 компонента из соответствующего семейства). Наличие такой шкалы даёт возможность сбалансированного получения уровней доверия со сложностью, сроками, стоимостью и самой возможностью их достижения.

Предполагается, что в ПЗ и ЗБ будут фигурировать или сами ОУД, или их усиления, полученные путём расширения требований (за счёт 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 OPE, OSE, OMA, 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 серьёзными. Его можно достичь без помощи разработчика и с минимальными затратами по средством анализа спецификации интерфейсов, эксплуатационной документации в сочетании с независимым тестированием.

ОУД.2, предусматривающий структурное тестированием и доступ к части проектной документации и результатам тестирования разработчиков приме-

ним, когда разработчикам или пользователям требуется независимо получаемый умеренный уровень доверия при отсутствии доступа к полной документации по разработке.

В дополнение 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 результатом тестирования разработчика, анализом стойкости функций безопасности и свидетельстве поиска явных уязвимостей.

Требуется наличие списка конфигураций объекта оценки с уникальной идентификацией элементов конфигурации 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 разработчики или пользователя требуется умеренный уровень доверия на основе всестороннего исследования объекта оценки и процесса его разработки. По сравнению с ОУД.2 сюда добавлено требования, которые предписывают разработчику создавать акт об испытаниях с учётом особенностей не только функциональной спецификации, но и проекта верхнего уровня, кроме того, требуется контроль среды разработки управления конфигурацией объекта оценки.

ОУД.4 предусматривающий систематическое проектирование, тестирование и просмотр позволяет достичь доверия максимально возможного при следовании общепринятой практики 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, проектами верхнего и нижнего уровней, а также подмножеством реализаций применения неформальной модели политики безопасности объекта оценки. Среды других дополнительных требований выделяют независимый анализ уязвимостей, демонстрирующий устойчивость к попыткам проникновения нарушителей с низким потенциалом нападения и автоматизацию управления конфигурацией. Отличительной особенностью ОУД.5 — это полуформальное проектирование и тестирование. С его помощью достигается доверие, максимально возможное при следовании строгой практики 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 ещё 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 путём 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 7 уровне дополнительно требуется:

- формальное представление функциональной спецификации проекта верхнего уровня и формальная демонстрация соответствия между ними;
- модульная, иерархическая и простая структура проект объекта оценки, добавление представления реализации как основы акта об испытаниях проекта;
- полное независимое подтверждение результатов тестирования разработчиком.

3.5. Основные понятия и идеи общей методологии и оценки (ОМО) безопасности ИТ. Входная и выходная задачи, задачи оценки

С целью унификации процедуры сертификации по ОК в августе 1999 года была опубликована общая методология оценки безопасности информационных технологий, описывающая минимальный набор действий при проведении оценки. Проекта ОК с самого начала носил не только технический, но и экономико-политический характер. Его цель состояла в частности в

том, чтобы упростить, удешевить и ускорить выход сертифицированных изделий ИТ на мировой рынок. Для этого в мае 2000 года уполномоченная правительственной организацией 6 стран основателей проекта ОК, а также Австралией, Новой Зеландией, Финляндией, Швецией, Грецией. . . подписали соглашение о признании сертификатов по ОК в области безопасности ОТ. Участие в соглашении предусматривает соблюдение 2 независимых условий:

- признание сертификатов, выданных соответствующими органами других стран-участниц;
- возможность осуществления подобной сертификации.

Очевидно, что от взаимного признания сертификатов выигрывают не только производители ИТ, но и потребители. Что же касается их выдачи, то соглашение предусматривает жёсткий контроль при получении и подтверждении этого права (например предусмотрено проведение т. н. теневых сертификационных испытаний под контролем независимых экспертов). Т. о. для полноценного участия в соглашении помимо желания государство должно располагать органами сертификации с достаточными ресурсами и штатом специалистов, квалификация которых получила официальное международное признание.