Тема 2.1 Общие критерии безопасности

1 Общие критерии – основные изменения

Рабочая группа 3 подкомиссии 27 Международной организации по стандартизации (ИСО) завершила разработку версии 2.0 «Общих критериев оценки безопасности информационных технологий».

Во второй версии Общих критериев сохранены основные концептуальные положения версии 1.0. Изменения коснулись структуры всего документа, некоторых классов, семейств и компонентов требований безопасности.

В версии 2.0 Общих критериев остались только три части:

часть 1 – «ПРЕДСТАВЛЕНИЕ И ОБЩАЯ МОДЕЛЬ»;

часть 2 – «ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ»;

часть 3 – «ТРЕБОВАНИЯ ГАРАНТИРОВАННОСТИ».

Часть 4 «ПРЕДОПРЕДЕЛЕННЫЕ ПРОФИЛИ ЗАЩИТЫ» вынесена за пределы проекта стандарта, что логично, учитывая постоянные дополнения каталога Профилей защиты.

В разделе «ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ» (часть 2) появились два новых класса: FCS («КРИПТОГРАФИЧЕСКАЯ ПОДДЕРЖКА») и FMT («УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ»).

Класс FCS был анонсирован еще в версии 1.0. Он включает два семейства: FCS_CKM («Управление криптографическими ключами») и FCS_COP («Криптографические операции»).

Класс FMT явился результатом перегруппировки требований, связанных с управлением безопасностью объекта оценки. В него вошли семейства: FMT_MOF («Управление функциями безопасности объекта оценки»), FMT_MSA («Управление признаками безопасности»), FMT_MTD («Управление данными функций безопасности»), FMT_REV («Аннулирование»), FMT_SAE («Истечение признака безопасности») и FMT_SMR («Функции управления безопасностью»).

Существенно изменились структура и содержание классов FAU («Аудит безопасности»), FDP («Защита данных пользователя») и FIA («Идентификация и аутентификация»).

В классе FAU исключено шесть семейств: FAU_MGT («Управление аудитом безопасности»), FAU_POP («Обработка сохраняемых данных аудита безопасности»), FAU_PRO («Защита трассы контроля безопасности»),FAU_PRP («Обработка данных аудита безопасности до хранения») – их требования сгруппированы в близких по назначению других модернизированных семействах этого же класса; FAU_PAD («Обнаружение аномалии по базовому образцу»), FAU_PIT («Средства идентификации проникновения») – их требования сгруппированы в модернизированном и дополненном еще двумя компонентами семействе FAU_SAA («Анализ аудита безопасности»).

В классе FDP исключены три семейства: FDP_ACI («Инициализация признаков объекта»), FDP_SAM («Модификация признаков безопасности»), FDP_SAQ («Запрос признака безопасности») - их требования сгруппированы в новом классе FMT, а также добавлено новое семейство FDP_DAV («Аутентификация данных»). Это семейство, состоящее из двух компонентов: FDP_DAU.1 («Базисная аутентификация данных») и FDP_DAU.2 («Аутентификация данных с идентификацией гаранта»), требует обеспечения гарантий проверки правильности специфицированного модуля данных, которые впоследствии могут быть использованы для проверки того, что, например, информация не была изменена или подделана. Это – своего рода нотаризация данных, но, в отличие от нотаризации при обмене данными в сетевых конфигурациях (класс FCO), применяемая для «статических» данных.

В классе FIA исключены семейства: FIA_ADA («Администрация данных аутентификации пользователей»), FIA_ADP («Защита данных аутентификации пользователей») и FIA_ATA («Администрирование признака пользователя») – их основные требования сгруппированы в соответствующих семействах нового класса FMT.

Незначительные изменения претерпели остальные классы функциональных требований.

В разделе «ТРЕБОВАНИЯ ГАРАНТИРОВАННОСТИ» (часть 3) в классе ADV («РАЗРАБОТКА») выделены в отдельное семейство ADV_SPM («Модель политики безопасности») требования к модели политики безопасности объекта оценки.

В классе ATE («ТЕСТИРОВАНИЕ») в семействе ATE_FUN («Функциональное тестирование») появился дополнительный компонент ATE_FUN.2 («Упорядоченное функциональное тестирование»), используемый в уровнях гарантии оценки УГО-6 и УГО-7 и требующий включения в тестовую документацию анализа последовательности процедур тестирования, входивших ранее в компонент ATE_COV.3.

В классе AVA («АНАЛИЗ УЯЗВИМОСТЕЙ») в семействе AVA_MSU («Неправильное применение») добавлен третий компонент, предусматривающий дополнительное выполнение Оценщиком независимого тестирования (типа атаки) для подтверждения идентификации в тестовой документации всех возможных опасных состояний. В семействе AVA_SOF («Сила функций безопасности объекта оценки») исключено описание ранжирования силы функции на «базовую», «среднюю» и «высокую» и введено требование оценки соответствия силы функции безопасности, заданной в Задании по безопасности или Профиле защиты.

В свою очередь, требования к Профилю защиты (класс APE) и Заданию по безопасности (класс ASE) теперь предусматривают необходимость включения в функциональные требования минимального уровня силы для функций безопасности, реализуемых механизмами случайной выборки или перестановки (например, паролирование или хэш-функции). Уровень определяется как «базовый», «средний» или «высокий» в зависимости от целей безопасности объекта оценки. Для некоторых целей безопасности возможно применение специфических метрик силы функции. Если в требованиях гарантированности используется уровень гарантии оценки УГО-1, который не включает компонента семейства AVA_SOF, сила функций безопасности в функциональных требованиях не задается.

Кроме того, в Профиле защиты предусмотрена возможность использования не только функциональных требований из части 2 Общих критериев, но, при необходимости, и обоснованных дополнительных требований.

В классе AGD («ДОКУМЕНТЫ РУКОВОДСТВА») в семействе AGD_ADM требования к Руководству администратора представлены в более общем виде.

Версия 2.0 «Общих критериев оценки безопасности информационных технологий» представлена в ИСО в качестве проекта международного стандарта. Официальный документ ИСО планируется к выпуску в первом полугодии 1999 года.

2 Общие критерии – заключение

«Критерии безопасности компьютерных систем» МО США явились первой попыткой создать единый стандарт безопасности, рассчитанный на разработчиков, потребителей и специалистов по сертификации компьютерных систем. «Оранжевая книга» послужила основой для разработчиков всех остальных стандартов информационной безопасности и до сих пор, с учетом дополнений и пояснений, используется в США в качестве руководящего документа при сертификации компьютерных систем обработки информации. Слабым местом «Оранжевой книги» является недостаточное внимание требованиям гарантии оценки.

В «Европейских критериях» впервые вводится понятие гарантированности и шкала для критериев гарантированности – уровни гарантии. «Европейские критерии» придают требованиям гарантированности даже большее значение, чем функциональным требованиям. «Европейские критерии» полностью принимают классы безопасности «Оранжевой книги» и вводят еще пять дополнительных классов.

«Канадские критерии оценки безопасности компьютерных систем» явились первым стандартом информационной безопасности, в котором на уровне структуры документа функциональные требования к средствам защиты отделены от требований гарантии оценки (адекватности реализации). В «Канадских критериях» отвергается подход к оценке уровня безопасности с помощью универсальной шкалы и используется независимое ранжирование требований по каждому разделу,

обеспечивающее гибкость в подходе к оценке безопасности различных типов изделий и систем.

«Федеральные критерии безопасности информационных технологий» являются по сравнению с «Оранжевой книгой» стандартом нового поколения. «Федеральные критерии» являются первым стандартом информационной безопасности, в котором определяются три независимые группы требований: функциональные требования к средствам защиты, требования к технологии разработки и к процессу квалификационного анализа(сертификации). Авторами стандарта впервые предложена концепция Профиля защиты – документа, содержащего описание всех требований безопасности как к самому продукту информационной технологии, так и к процессу его проектирования, разработки, тестирования и квалификационного анализа. Разработчики «Федеральных критериев» также отказались от используемого в «Оранжевой книге» подхода к оценке уровня безопасности изделия ИТ на основе обобщенной универсальной шкалы классов безопасности. Вместо этого предлагается независимое ранжирование требований каждой группы, т.е. используется множество частных шкал-критериев, характеризующих обеспечиваемый уровень безопасности. Такой подход позволяет разработчикам и потребителям изделия ИТ выбрать наиболее приемлемое решение и определить необходимый и достаточный набор требований для каждого конкретного продукта ИТ и среды его эксплуатации.

«Общие критерии оценки безопасности информационных технологий» представляют собой результат обобщения всех достижений в области информационной безопасности. Они согласованы с существующими стандартами и развивают их путем введения новых концепций, соответствующих современному уровню развития информационных технологий. «Общие критерии» продолжили подход «Федеральных критериев», направленный на отказ от единой шкалы классов безопасности, и повысили гибкость и удобство применения критериев путем введения частично упорядоченных шкал. Предложенные в «Общих критериях» структуры Профиля защиты и Задания по безопасности позволяют потребителям и производителям (разработчикам) в полной мере выразить свой взгляд на требования

безопасности и задачи защиты, а с другой стороны дают возможность оценщикам проанализировать взаимное соответствие между требованиями потребителей, задачами и средствами защиты продукта ИТ. По уровню систематизации, полноте и степени детализации требований «Общие критерии» оставили далеко позади все существующие стандарты безопасности информационных технологий. При сравнительном анализе всех основных стандартов безопасности ИТ по пяти показателям (универсальность, гибкость, гарантированность, реализуемость, актуальность) «Общие критерии» получили наивысшую оценку. «Общие критерии» разрабатываются как проект международного стандарта ИСО и должны позволить осуществлять сертификацию продуктов ИТ на глобальном уровне.

Тема 2.2 Общие критерии безопасности – история; общая модель

1 История вопроса

Общие критерии представляют собой результат усилий по разработке критериев оценки безопасности информационных технологий (ИТ), которые широко используются в международном сообществе. Они согласуют и развивают целый ряд исходных критериев, а именно существующие европейские, американские и канадские критерии (ITSEC, TCSEC и CTCPEC соответственно). В Общих критериях устранены концептуальные и технические различия между исходными документами. Это является существенным вкладом в разработку международного стандарта и открывает путь к всеобщему взаимному признанию результатов оценок.

Критерии, разработанные в Канаде и европейских странах, следовали логике основополагающей американской работы TCSEC («Оранжевой книги»). Разработка в США Федеральных критериев была первой попыткой объединения различных критериев с TCSEC, приведшей, в конце концов, к существующему объединению ресурсов для создания Общих критериев.

Наиболее сильной стороной при разработке ОК было привлечение всех, кто имел опыт создания оригинальных национальных критериев. Для ОК было полезно объединение их знаний и их намерение обеспечить максимально гибкий подход к стандартизации функциональных возможностей безопасности и оценочного доверия к безопасности. Общие критерии обладают достаточной адаптивностью, дающей возможность их эволюционного внедрения в многочисленные существующие национальные системы оценки безопасности, сертификации и аттестации ИТ.

Структура ОК также обеспечивает значительную гибкость при спецификации безопасных продуктов. Потребители и другие заинтересованные стороны могут задать функциональные возможности безопасности продукта с использованием стандартных профилей защиты и самостоятельно выбрать оценочный уровень доверия к безопасности из предопределенной совокупности семи возрастающих оценочных уровней доверия, от ОУД1 до ОУД7.

Версия 1.0 ОК была опубликована для обсуждения в январе 1996 г. Версия 2.0, учитывающая итоги широкого обсуждения и двухлетний опыт применения версии 1.0, была опубликована в мае 1998г.

Версия 2.0 ОК была принята Международной организацией по стандартизации (ISO) в качестве финального рабочего проекта, на основе которого был принят Международный стандарт ISO/IEC 15408–99 «Критерии оценки безопасности информационных технологий», введенный в действие с 1 декабря 1999 г.

2 Общая модель

ОК содержат требования безопасности ИТ, предъявляемые к продуктам или системам и относящиеся к различаемым категориям функциональных требований (Часть 2 ОК) и требований доверия к безопасности (Часть 3 ОК). Функциональные требования ОК определяют желательный режим безопасности. Требования доверия являются основой для уверенности в том, что заявленные меры безопасности эффективны и корректно реализованы.

Версия 2.0 Общих критериев состоит из трех частей. Описание полезности каждой части для заинтересованных лиц трех категорий (потребителей, разработчиков и оценщиков) показано ниже.

Подход.

Доверие к безопасности ИТ может быть достигнуто посредством действий, предпринимаемых в процессе разработки, оценки и эксплуатации.

Разработка.

Общие критерии определяют общепризнанную совокупность требований к ИТ, которые могут быть использованы при установлении требований безопасности для будущих продуктов и систем. ОК также определяют профиль защиты (ПЗ) как конструкцию, позволяющую потребителям и разработчикам создавать стандартизованные наборы требований безопасности, отвечающие их потребностям.

Объект оценки (ОО) – это та часть продукта или системы, которая является предметом оценки. Угрозы, цели и требования безопасности ОО, а также краткая спецификация функций безопасности и мер доверия к безопасности излагаются в

задании по безопасности (ЗБ), которое используется оценщиками как основание при оценке.

Оценка.

Основными исходными материалами для оценки являются задание по безопасности, совокупность свидетельств об ОО и собственно ОО. Ожидаемым результатом процесса оценивания является содержащееся в одном или нескольких отчетах, документирующих заключения оценки, подтверждение того, что ОО удовлетворяет требованиям ЗБ.

Таблица 1 – Описание полезности общих критериев

Потребители	**Разработчики**	**Оценщики**	
Часть 1: Введение и общая модель	Общие сведения по применению. Руководство по структуре профилей защиты	Общие сведения и справочное руководство по разработке требований и формулированию спецификаций безопасности для объектов оценки	Общие сведения по применению. Руководство по структуре профилей защиты и заданий по безопасности
Часть 2: Функциональные требования безопасности	Руководство и справочник при формулировании требований к функциям безопасности	Справочник по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки	Обязательное изложение критериев оценки, используемых при определении эффективности выполнения объектом оценки заявленных функций безопасности
Часть 3: Требования доверия к безопасности	Руководство по определению требуемого уровня доверия	Справочник по интерпретации требований доверия и определению подходов к установлению доверия к объектам оценки	Обязательное изложение критериев оценки, используемых при определении доверия к объектам оценки и оценке профилей защиты и заданий по безопасности

Эксплуатация.

Во время эксплуатации ОО могут проявляться неизвестные ранее уязвимости, или же могут требовать пересмотра предположения в отношении среды. Тогда разработчику может быть предложено внести изменения в ОО. Вследствие этих изменений может потребоваться переоценка.

Основы безопасности.

В ОК вопросы безопасности обсуждаются с использованием иерархической структуры понятий безопасности:

Среда безопасности.

Законы, политики безопасности организаций и пр., определяющие условия использования ОО. Сюда также включены угрозы, относящиеся к среде ОО.

Цели безопасности.

Сформулированное намерение противостоять идентифицированным угрозам и/или удовлетворять принятой политике безопасности организации и предположениям.

Требования безопасности ОО.

Преобразование целей безопасности ИТ в совокупность специальных требований к функциям безопасности и требований доверия к безопасности, относящихся к ОО и его среде ИТ.

Спецификации безопасности ОО.

Определяют фактически существующую или предполагаемую реализацию ОО.

Реализация ОО.

Воплощение ОО в соответствии с его спецификацией.

Тема 2.3 Общие критерии безопасности – ключевые понятия; доверие к безопасности

1 Общие положения

Стандарт ISO/IEC 15408 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (введен в действие 1 декабря 2013 года) – самый полный и современный стандарт.

По историческим причинам данный стандарт часто называют «Общими критериями» (или даже ОК). Мы также будем использовать это сокращение.

«Общие критерии» на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от «Оранжевой книги», ОК не содержат предопределенных «классов безопасности». Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные «программы» – задания по безопасности, типовые профили защиты и пр. Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, «с нуля», программы не пишут уже очень давно; оценка безопасности тоже вышла на сопоставимый уровень сложности, и «Общие критерии» предоставили соответствующий инструментарий.

Важно отметить, что требования могут быть параметризованы, как и полагается библиотечным функциям.

Как и «Оранжевая книга», ОК содержат два основных вида требований безопасности:

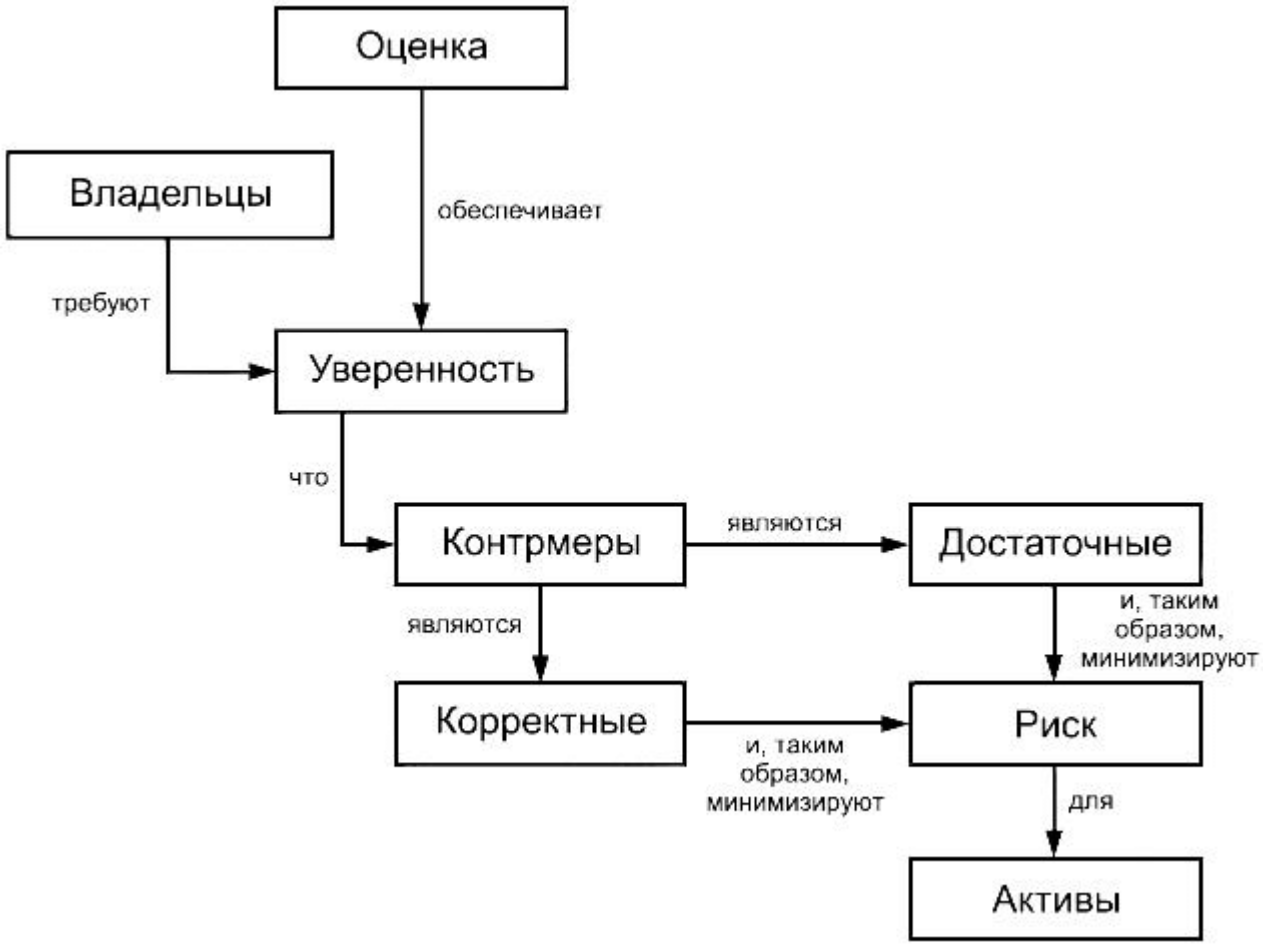

Рисунок 1 – Понятия, используемые при оценке, и их взаимосвязь

– функциональные, 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 предъявляются, а их выполнение проверяется для определенного объекта оценки (ОО) - совокупности программного, программно-аппаратного и/или аппаратного обеспечения, возможно сопровождаемая руководствами.

На рисунке 1 представлена взаимосвязь понятий, используемых при оценке и их взаимосвязь

По стандарту ИСО/МЭК 15408 признают два типа оценки: оценка ЗБ/ОО и оценка ПЗ, которая определяется в ИСО/МЭК 15408-3.

Профиль защиты - независимое от реализации изложение потребностей в безопасности для некоторого типа ОО.

Задание по безопасности - зависимое от реализации изложение потребностей в безопасности для конкретного идентифицированного ОО.

По ИСО/МЭК 15408 оценка ЗБ/ОО проходит в два этапа:

– оценка ЗБ: на этом этапе определяют достаточность ОО и среды функционирования;

– оценка ОО: на этом этапе определяют корректность ОО; как отмечалось ранее, оценка ОО не включает оценку корректности среды функционирования.

Оценку ЗБ выполняют путем применения критериев оценки заданий по безопасности (которые определены в разделе ASE ИСО/МЭК 15408-3). Конкретный способ применения критериев ASE определяется используемой методологией оценки.

В то время как ЗБ всегда описывает конкретный ОО (например, межсетевой экран X-2, версия 3.1), ПЗ предназначен для описания типа ОО (например, межсетевые экраны прикладного уровня). Поэтому один и тот же ПЗ можно использовать в качестве шаблона для множества различных ЗБ, которые будут использовать в различных оценках. Подробное описание ПЗ приведено в приложении В.

Обычно ЗБ описывает требования для ОО и его формирует разработчик ОО, в то время как ПЗ описывает общие требования для некоторого типа ОО и поэтому обычно разрабатывается:

– сообществом пользователей, стремящихся прийти к консенсусу относительно требований для данного типа ОО;

– разработчиком ОО или группой разработчиков подобных ОО, желающих установить минимальный базис для конкретного типа ОО;

– правительственной организацией или крупной корпорацией, определяющими свои требования как часть процесса закупки.

Задание по безопасности либо соответствует рассматриваемому ПЗ, либо не соответствует. ИСО/МЭК 15408 не признает "частичное" соответствие. В стандарте приведены содержания ПЗ и ЗБ.

В ОК нет готовых классов защиты. Сформировать классификацию в терминах «Общих критериев» – значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

На основе ГОСТ Р 15408 ФСТЭК сформировала профили для систем антивирусной защиты и систем обнаружения вторжений. Профили представляют из себя наборы «деталей» ГОСТ Р 15408. Сами «детали» в терминологии ГОСТ 15408 называются компонентами, которые систематизированы в семейства, а те в свою очередь составляют классы. ГОСТ Р 15408 Часть 2 «Функциональные требования» содержит 11 классов, 66 семейств и 135 компонентов, а ГОСТ Р 15408 Часть 3 «Требования доверия» - 8 классов, 44 семейства, 93 компонента. Компоненты могут состоять из нескольких элементов, но компоненты неделимы при формировании профилей защиты и заданий по безопасности.

2 Ключевые понятия

1) Профиль защиты (ПЗ).

Профиль защиты определяет независимую от реализации совокупность требований и целей безопасности для некоторой категории продуктов или систем, отвечающую одинаковым запросам потребителей в безопасности ИТ. ПЗ предназначен для неоднократного применения и определения требований, которые признаны полезными и эффективными для достижения установленных целей.

Уже разработаны ПЗ для межсетевых экранов, реляционных баз данных и пр., а также для обеспечения обратной совместимости с классами B1 и C2 из TCSEC.

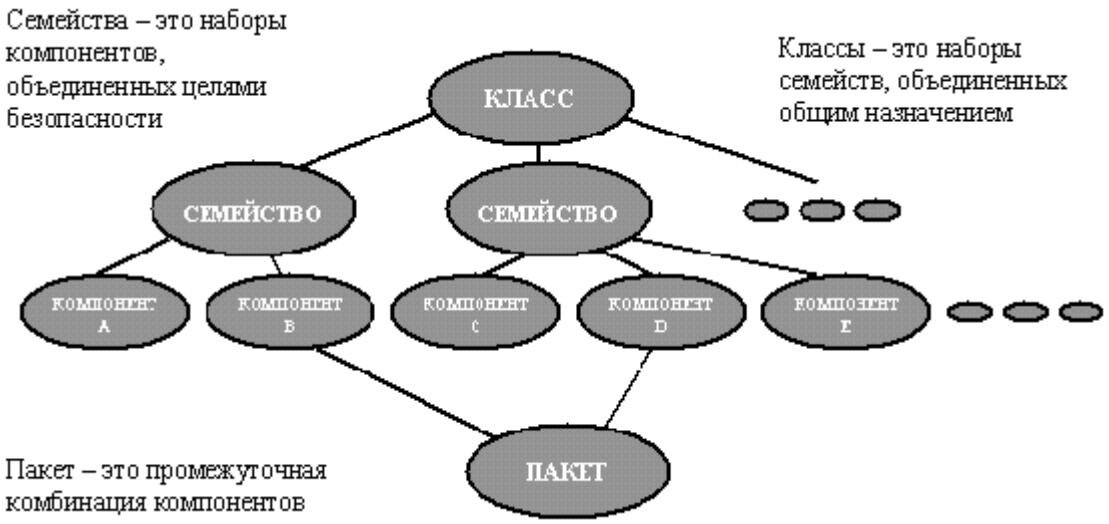

Рисунок 2 – Структура ключевых понятий

2) Задание по безопасности (ЗБ).

Задание по безопасности содержит цели и требования безопасности ИТ для конкретно определенного ОО и определяет функции безопасности и меры доверия, предоставляемые этим ОО для выполнения установленных требований. В ЗБ может быть заявлено о соответствии одному или нескольким ПЗ, и оно составляет основу для оценки.

3) Пакет.

Пакет позволяет выразить совокупность требований, которая соответствует некоторому подмножеству целей безопасности. Пакет предназначен для неоднократного применения и определения требований, которые признаны полезными и эффективными для достижения установленных целей. Пакет может использоваться для построения более объемных пакетов, ПЗ и ЗБ.

4) Компоненты.

ОК определяют совокупность конструкций, которые разделяют требования безопасности на взаимосвязанные наборы, называемые компонентами.

5) Операции на компонентах.

Компоненты ОК могут либо применяться прямо в том виде, в котором они определены в ОК, либо модифицироваться с использованием разрешенных операций для осуществления конкретной политики безопасности или противостояния

определенной угрозе. Для каждого компонента устанавливаются и определяются разрешенные операции, условия их применения и результаты применения. К разрешенным операциям относятся итерация, назначение, выбор и уточнение.

6) Зависимости компонентов

Между компонентами могут существовать зависимости. Зависимости возникают, когда компонент не самодостаточен и зависит от наличия другого компонента. Зависимости могут существовать между функциональными компонентами, между компонентами требований доверия, а также, в редких случаях, между теми и другими. В каждом компоненте указываются зависимости, которые необходимо удовлетворить при его применении.

7) Соглашение о наименовании компонентов

Требования к ОО могут быть составлены на основе иерархии спецификаций. Имя класса состоит из трех букв (например, FMT). Имена семейств внутри каждого класса получают, добавляя к имени класса символ подчеркивания и еще три буквы (например, FMT_SMR). Нумеруются как компоненты внутри семейств (например, FMT_SMR.2), так и элементы внутри компонентов (например, FMT_SMR.2.1).

На диаграмме показана таксономия семейства на примере семейства FAU_APR «Автоматическая реакция аудита безопасности». Оно содержит три компонента, причем компоненты 1 и 2 иерархически зависимы.

На диаграмме показана таксономия семейства на примере семейства FAU_APR «Автоматическая реакция аудита безопасности». Оно содержит три компонента, причем компоненты 1 и 2 иерархически зависимы.

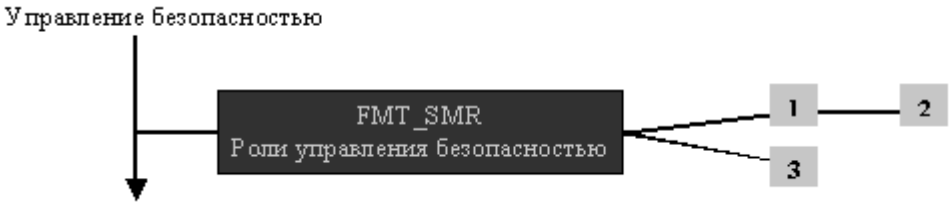

Рисунок 3 – Пример семейства

8) Цели таксономии.

При определении требований безопасности для доверенных продуктов и систем пользователь/разработчик должен рассмотреть угрозы, относящиеся к среде ИТ. ОК содержат каталог компонентов, с которым разработчики ПЗ и ЗБ могут сверяться при формулировании требований безопасности. Иерархическая организация этих компонентов помогает пользователю ОК находить подходящие компоненты для противостояния угрозам. Затем пользователь включает требования безопасности в профили защиты и задание по безопасности для ОО.

9) Функциональные компоненты.

Функциональные компоненты безопасности применяются для выражения широкого спектра функциональных требований безопасности в составе ПЗ или ЗБ. Компоненты являются упорядоченными совокупностями функциональных элементов и объединены, как указано выше, в семейства с общими целями (например, «Защита журнала аудита безопасности») и классы с общим назначением (например, «Аудит»). Между функциональными компонентами может существовать иерархия.

10) Расширяемость компонентов.

ОК допускают применение иных функциональных компонентов, помимо приведенных в части 2. Часть 3 содержит требования по оценке подобных компонентов. Следует заметить, что применение подобных расширений может потребовать предварительного одобрения органа сертификации.

11) Каталог компонентов.

Часть 2 ОК содержит каталог функциональных компонентов. Ниже в самом общем виде представлен обзор всех одиннадцати функциональных классов из версии 2.0 ОК. Существуют некоторые зависимости между классами, например,

эффективность классов защиты данных зависит от правильного выполнения требований идентификации и аутентификации пользователей. Классы перечислены по алфавиту (латинскому).

12) Аудит (FAU).

Аудит безопасности включает распознавание, запись, хранение и анализ информации, связанной с действиями, влияющими на безопасность. Получаемые в результате записи аудита могут быть проанализированы для определения значимости этих действий для безопасности. Этот класс образован из семейств, которые определяют, помимо всего прочего, требования к отбору событий, потенциально подвергаемых аудиту, анализу записей аудита, их защите и хранению.

13) Связь (FCO).

Этот класс содержит два семейства, связанные с подтверждением идентификаторов сторон, участвующих в обмене данными. Эти семейства связаны с неотказуемостью (невозможностью отказаться от) данных со стороны отправителя и получателя.

14) Криптографическая поддержка (FCS).

Этот класс применяется, когда в ОО реализованы криптографические функции. Они могут использоваться, например, для поддержки связи, идентификации и аутентификации, а также разделения данных. В двух семействах рассматривается их применение (в самом общем виде) и управление криптографическими ключами.

15) Защита данных пользователя (FDP).

Этот класс содержит семейства, которые устанавливают требования, относящиеся к защите данных пользователя. Требования этих семейств относятся к данным пользователя в пределах ОО при их импорте, экспорте и хранении, а также к атрибутам безопасности, непосредственно связанным с этими данными.

16) Идентификация и аутентификация (FIA).

Требования к идентификации и аутентификации обеспечивают однозначную идентификацию уполномоченных пользователей и правильную ассоциацию атрибутов безопасности с пользователями и субъектами. Семейства этого класса посвящены определению и верификации идентичности пользователей, определению их полномочий по взаимодействию с ОО, а также правильной ассоциации атрибутов безопасности с уполномоченными пользователями.

17) Управление безопасностью (FMT).

Этот класс применяется для спецификации управления атрибутами безопасности, данными и функциями безопасности ОО. Могут быть определены различные роли управления и распределение обязанностей между ними. Класс применяется для охвата аспектов управления из других функциональных классов.

18) Приватность (FPR).

Требования класса «Приватность» направлены на защиту пользователя от раскрытия его идентичности и злоупотребления этим другими пользователями. Семейства этого класса связаны с анонимностью, применением псевдонимов, невозможностью ассоциации и скрытностью.

19) Защита ФБО (FPT).

Этот класс сосредоточен на защите данных ФБО, но не данных пользователей. Он связан с целостностью данных ФБО и управлением данными и механизмами ФБО.

20) Использование ресурсов (FRU).

Класс «Использование ресурсов» содержит три семейства, которые поддерживают доступность требуемых ресурсов, таких как вычислительные возможности (возможности процессора) и объем памяти. Семейства детализируют требования к отказоустойчивости, приоритетам обслуживания и распределению ресурсов.

21) Доступ к ОО (FTA).

Этот класс устанавливает требования к управлению открытием сеанса пользователя, дополняя установленные требования идентификации и аутентификации. Требования по доступу к ОО регулируют такие детали, как ограничение возможного количества сеансов пользователя и их видов, отображение истории доступа, и модификация параметров доступа.

22) Доверенный маршрут/канал (FTP).

В семействах этого класса рассматриваются доверенные маршруты связи как между пользователями и ФБО, так и между ФБО. Доверенные маршруты составляют из доверенных каналов, которые имеются для связей между ФБО; они предоставляют пользователям способ выполнения функций путем прямого взаимодействия с ФБО. Пользователь или ФБО могут инициировать обмен, гарантирующий защиту от модификации недоверенными приложениями.

3 Доверие к безопасности

1) Таксономия

Требования доверия к безопасности определены в части 3 ОК. Таксономия требований доверия подобна принятой для функциональных требований. Часть 3 содержит два класса, в которых приведены требования доверия для оценки ПЗ и ЗБ, семь классов, из которых можно выбирать требования доверия непосредственно для оценки ОО, а также класс, посвященный поддержанию доверия после оценки ОО. Эти десять классов аннотированы ниже.

2) Оценка ПЗ и ЗБ

Для оценки ПЗ и ЗБ предназначены классы требований доверия APE и ASE соответственно. Все требования этих классов предназначены для применения при оценке ПЗ и ЗБ. Их применение предусмотрено для выяснения того, является ли ПЗ или ЗБ значимым основанием для оценки ОО.

3) Оценка профиля защиты (APE)

Цель оценки ПЗ состоит в том, чтобы показать, что ПЗ является полным, непротиворечивым и технически грамотным. В дальнейшем применение ПЗ

предусмотрено при изложении требований к оцениваемому ОО. Семейства этого класса связаны со средой безопасности, целями безопасности и требованиями безопасности ОО.

4) Оценка задания по безопасности (ASE)

Цель оценки ЗБ состоит в том, чтобы показать, что ЗБ является полным, непротиворечивым и технически грамотным, и поэтому оно пригодно в качестве основы для оценки ОО. Требования семейств этого класса связаны со средой безопасности, целями безопасности, утверждениями о соответствии ПЗ, требованиями безопасности ОО и краткой спецификацией ОО.

5) Классы требований доверия при оценке ОО

Классы перечислены по алфавиту (латинскому)

6) Управление конфигурацией (ACM)

Класс «Управление конфигурацией» содержит требования по адекватному сохранению целостности ОО. В частности, управление конфигурацией предоставляет уверенность в том, что оцениваются именно те ОО и документация, которые подготовлены к распространению. Семейства данного класса связаны с возможностями, областью и автоматизацией управления конфигурацией.

7) Поставка и эксплуатация (ADO)

Этот класс содержит семейства, связанные с мерами, процедурами и стандартами для безопасной поставки, инсталляции и эксплуатации ОО, обеспечивая, чтобы безопасность ОО не нарушалась при их выполнении.

8) Разработка (ADV)

Семейства этого класса связаны с преобразованием ФБО от спецификации до реализации и отображением в них требований вплоть до самого нижнего уровня представления.

9) Руководства (AGD)

Класс «Руководства» связан с безопасной эксплуатацией ОО пользователями и администраторами.

10) Поддержка жизненного цикла (ALC)

Требования семейств данного класса связаны с жизненным циклом ОО, включая определение жизненного цикла, инструментальные средства и методы, безопасность разработки и устранение недостатков, обнаруженных потребителями ОО.

11) Тестирование (ATE)

Этот класс связан с демонстрацией того, что ОО удовлетворяет функциональным требованиям. В его семействах рассматриваются вопросы покрытия и глубины тестирования разработчиком, а также требования к независимому тестированию при оценке.

12) Оценка уязвимостей (AVA)

Данный класс определяет требования, направленные на идентификацию уязвимостей, возможных для использования, которые могут быть внесены при проектировании, эксплуатации, неправильном применении или неправильном конфигурировании ОО. В семействах, сосредоточенных здесь, для исследования выявленных уязвимостей применяются анализ скрытых каналов, анализ конфигурации ОО, проверка стойкости механизмов функций безопасности и идентификация недостатков, внесенных при разработке ОО.

13) Класс поддержания доверия

В этом классе представлены требования, которые предназначены для применения после завершения сертификации ОО согласно ОК. Эти требования нацелены на обеспечение того, что ОО продолжает удовлетворять своему ЗБ после изменений в ОО или в его среде. Класс содержит четыре семейства. В первом рассматривается содержание плана поддержания доверия, в котором отражается сущность предполагаемых изменений, средства контроля над ними, а также условия необходимости переоценки. Второе семейство посвящено категорированию компонентов ОО по их отношению к безопасности. Третье и четвертое охватывают анализ влияния изменений на безопасность и предоставление свидетельств следования процедурам поддержки.

Класс содержит необходимые материалы для построения системы поддержания доверия.

Таблица 2 – Назначение и применимость оценочных уровней доверия

Задача обратной совместимости: ОУД из ОК разработаны в целях сохранения концепций доверия, вытекающих из исходных критериев, таким образом, чтобы остались применимыми результаты предыдущих оценок. Таблица дает общее представление об эквивалентности, но следует помнить, что точного соответствия не существует, так как различаются подходы к установлению доверия.	**Общие критерии**	**Американские TCSEC**	**Европейские ITSEC**
	ОУД0	D: Минимальная защита	E0
	ОУД1		
	ОУД2	C1: Дискреционная защита	E1
	ОУД3	C2: Защита контролируемого доступа	E2
	ОУД4	B1: Меточная защита	E3
	ОУД5	B2: Структурированная защита	E4
	ОУД6	B3: Домены безопасности	E5
	ОУД7	A1: Верифицированный проект	E6

14) Оценочные уровни доверия

ОК содержат совокупность предопределенных уровней доверия, составленных из компонентов семейств доверия. Эти уровни предназначены как для достижения частичной обратной совместимости с исходными критериями, так и для обеспечения потребителя внутренне согласованными пакетами компонентов требований доверия с широкой областью применения. Иное группирование компонентов не исключается. Для достижения конкретных целей уровень доверия может быть усилен одним или несколькими дополнительными компонентами.

Уровни доверия определяют шкалу для сопоставления критериев оценки, содержащихся в ПЗ и ЗБ. Оценочные уровни доверия (ОУД) составлены из компонентов требований доверия одного ранга. Каждое семейство требований доверия вносит вклад в достижение ОО заявленного уровня безопасности. ОУД образуют возрастающую шкалу, которая позволяет соотнести полученный уровень доверия со стоимостью и возможностью достижения этой степени доверия. Имеются семь иерархически упорядоченных ОУД. Повышение доверия от уровня к уровню достигается заменой какого-либо компонента требований доверия иерархически более высоким компонентом из того же семейства (компоненты в семействах доверия всегда связаны иерархически) и добавлением компонентов требований доверия из других семейств.

15) Предопределенными ОУД являются:

– ОУД1 – предусматривающий функциональное тестирование;

– ОУД2 – предусматривающий структурное тестирование;

– ОУД3 – предусматривающий методическое тестирование и проверку;

– ОУД4 – предусматривающий методическое проектирование, тестирование и просмотр;

– ОУД5 – предусматривающий полуформальное проектирование и тестирование;

– ОУД6 – предусматривающий полуформальную верификацию проекта и тестирование;

– ОУД7 – предусматривающий формальную верификацию проекта и тестирование.

Тема 2.4 Общие критерии безопасности – оценочные уровни доверия; подход к оценке

1 Оценочные уровни доверия

Здесь аннотирован каждый из семи оценочных уровней доверия. ОУД1 является начальным уровнем. На уровнях до ОУД4 повышается строгость и детализация, но не применяются узко специализированные методы проектирования безопасности. Четыре первых уровня в основном применяются к уже существующим продуктам и системам.

Выше ОУД4 требуется расширение применения специализированных методов проектирования безопасности. Чтобы ОО отвечал требованиям этих уровней доверия, они должны учитываться непосредственно при проектировании и разработке ОО. На завершающем ОУД7 имеются значительные ограничения возможности выполнения требований вследствие как существенного влияния необходимых затрат на действия разработчика и оценщика, так и того, что самый простой из продуктов является, скорее всего, слишком сложным для применения известных в настоящее время методов формального анализа.

ОУД1 – предусматривающий функциональное тестирование

ОУД1 применим, когда требуется некоторая уверенность в правильном функционировании, а угрозы безопасности не рассматриваются как серьезные. Он будет полезен там, где требуется независимо полученное доверие к безопасности, подтверждающее заявление о том, что было уделено должное внимание защите персональных данных и подобной информации.

Этот уровень обеспечивает оценку ОО в том виде, в каком ОО доступен потребителю, путем независимого тестирования спецификаций и экспертизы представленной документации. Предполагается, что оценка на ОУД1 может успешно проводиться без помощи разработчика ОО и с минимальными затратами. Оценка на этом уровне должна предоставить свидетельство того, что ОО функционирует в соответствии с документацией и предоставляет требуемую защиту против идентифицированных угроз.

ОУД2 – предусматривающий структурное тестирование

ОУД2 содержит требование сотрудничества с разработчиком для получения информации о проекте и результатах тестирования, но не должен требовать со стороны разработчика усилий больших, чем это соответствует обычной коммерческой практике. Следовательно, не требуется существенного увеличения стоимости или затрат времени.

ОУД2 применим в тех случаях, когда разработчикам или пользователям требуется невысокий до умеренного независимо получаемый уровень доверия при отсутствии доступа к полной документации по разработке. Такая ситуация может возникать при обеспечении безопасности разработанных в прошлом систем или при ограниченной доступности разработчика.

ОУД3 – предусматривающий методическое тестирование и проверку

ОУД3 позволяет добросовестному разработчику получить максимум доверия путем надлежащего проектирования безопасности без значительного изменения существующей практики разработки. Он применим при требовании независимого получения умеренного уровня доверия на основе всестороннего исследования ОО и процесса его разработки без существенных затрат на изменение технологии проектирования.

Оценка на ОУД3 предусматривает анализ на основе тестирования «серого ящика», выборочного независимого подтверждения тестирования, выполненного разработчиком, и свидетельства поиска разработчиком явных уязвимостей. Также требуются контроль среды разработки и управление конфигурацией ОО.

ОУД4 – предусматривающий методическое проектирование, тестирование и просмотр

ОУД4 позволяет разработчику получить максимум доверия путем надлежащего проектирования безопасности, основанного на хорошей коммерческой практике разработки, которая при своей строгости не требует глубоких специальных знаний, навыков и других ресурсов. ОУД4 – самый высокий уровень, на который, вероятно, экономически целесообразно ориентироваться для существующих типов продуктов.

Он применим, когда разработчикам или пользователям требуется независимо получаемый уровень доверия от умеренного до высокого в ОО общего назначения и имеется готовность нести дополнительные, связанные с безопасностью производственные затраты.

Оценка на ОУД4 предусматривает анализ с использованием проекта нижнего уровня модулей ОО, а также подмножества реализации. Тестирование поддерживается независимым поиском явных уязвимостей. При управлении разработкой применяются модель жизненного цикла, идентификация инструментальных средств и автоматизированное управление конфигурацией.

ОУД5 – предусматривающий полуформальное проектирование и тестирование

ОУД5 позволяет разработчику получить максимум доверия путем проектирования безопасности, основанного на строгой коммерческой практике разработки, поддержанной умеренным применением узко специализированных методов проектирования безопасности. При проектировании и разработке такого ОО, по-видимому, должна учитываться необходимость достижения ОУД5. Вероятно, дополнительные затраты, сопутствующие требованиям ОУД5 относительно строгой разработки, не будут большими без учета применения узко специализированных методов. ОУД5 применим при требовании независимо получаемого высокого уровня доверия для запланированной разработки со строгим подходом к разработке без внесения излишних затрат на применение специализированных методов проектирования безопасности.

Оценка на ОУД5 предусматривает анализ, который охватывает всю реализацию. Доверие к безопасности обеспечивается применением формальной модели и полуформального представления функциональной спецификации и проекта верхнего уровня, а также полуформального показа соответствия. Поиск уязвимостей должен обеспечить уверенность в стойкости к атакам нарушителей с умеренным потенциалом нападения. Необходимо проведение анализа тайных каналов, а также модульное построение ОО.

ОУД6 – предусматривающий полуформальную верификацию проекта и тестирование

ОУД6 позволяет разработчикам получить высокое доверие к безопасности путем применения узко специализированных методов проектирования безопасности в строго контролируемой среде разработки при производстве высококачественных продуктов для защиты высоко оцениваемых активов от значительных рисков. Поэтому ОУД6 применим при разработке ОО, специализированных на обеспечении безопасности, для применения в ситуациях высокого риска, где ценность защищаемых активов оправдывает дополнительные затраты.

Оценка на ОУД6 предусматривает анализ, поддержанный модульным и иерархическим (по уровням детализации) подходом к проектированию, а также структурированным представлением реализации. Независимый поиск уязвимостей должен обеспечить уверенность в стойкости к атакам нарушителей с высоким потенциалом нападения. Поиск тайных каналов должен быть систематическим. Привлекаются более мощные средства управления средой разработки и конфигурацией.

ОУД7 – предусматривающий формальную верификацию проекта и тестирование

ОУД7 применим при разработке безопасных ОО для применения в ситуациях чрезвычайно высокого риска и/или там, где высокая ценность активов оправдывает более высокие затраты. Практическое применение ОУД7 в настоящее время ограничено ОО, которые предназначены преимущественно для реализации функций безопасности и поддаются подробному формальному анализу.

Для оценки на ОУД7 формальная модель дополняется формальным представлением функциональной спецификации, проекта верхнего уровня и соответствия между ними. Требуются свидетельство тестирования разработчиком «белого ящика» и полное независимое подтверждение всех результатов тестов, выполненных разработчиком. Сложность проекта должна быть минимизирована.

2 Подход к оценке

Процесс оценки может происходить одновременно с разработкой ОО или следовать за ней. Основным исходным материалом для оценки является ЗБ, описывающее функции безопасности ОО, которое, в свою очередь, может ссылаться на один или несколько ПЗ, соответствие с которыми заявляется. Ниже определен подход к описанию в ПЗ и ЗБ функциональных возможностей безопасности ОО.

1) Профиль защиты.

ПЗ описывает независимые от реализации наборы требований безопасности для определенных категорий ОО и формулирует проблему безопасности, для решения которой предназначен соответствующий продукт. В ПЗ указываются компоненты функциональных требований и требований доверия, включая ОУД, и представляется логическое обоснование для выбранных компонентов. В ПЗ выделяются следующие разделы.

2) Введение.

Содержит информацию, необходимую при использовании реестра ПЗ. К ней относятся маркировка и аннотация, которая может применяться отдельно.

3) Описание ОО.

Устанавливает контекст оценки. Поскольку рассматривается определенная категория ОО, могут быть указаны совокупность предположений и условия применения ОО этой категории.

4) Среда безопасности.

В повествовательной форме приводится формулировка проблемы безопасности, решаемой ОО. Описываются аспекты безопасности среды, в которой предполагается применение ОО. Описание включает:

– предположения: аспекты безопасности среды, в которой предполагается применение ОО, включая аспекты физического окружения, персонала и внешних связей;

– угрозы: прогнозируемые угрозы активам ИТ, в том числе те, которым не противостоит собственно ОО. В описании угрозы указываются источник, способ и предмет нападения;

– политику безопасности организации: правила, которым ОО должен подчиняться.

5) Цели безопасности.

Отражают заявленное намерение противостоять идентифицированным угрозам и/или соответствовать политике безопасности организации. Включают цели, относящиеся как к ОО, так и к его среде; все они должны быть сопоставлены с конкретными угрозами, политикой или предположениями.

6) Требования безопасности ИТ.

Описывают функциональные требования и требования доверия для ОО. Функциональные требования обычно берутся из части 2 ОК. Требования доверия входят в состав компонентов из части 3 ОК и могут иметь вид предопределенного пакета (например, ОУД), дополнительно усиленного другими компонентами требований доверия из части 3. В некоторых случаях требования могут быть расширены включением компонентов требований, не входящих в ОК, с необходимым обоснованием. Дополнительно может быть включено описание требований безопасности для среды ИТ. (Последнее может быть опущено, если объектом оценки являются самодостаточные ФБО, не связанные с какими-либо утверждениями о среде ИТ).

7) Обоснование.

Состоит из двух подразделов:

– обоснование целей демонстрирует, что цели безопасности охватывают все выявленные аспекты среды, обеспечивая их полное покрытие;

– обоснование требований демонстрирует пригодность требований безопасности для достижения целей безопасности.

8) Задание по безопасности.

ЗБ является основой для соглашения между разработчиками, потребителями, оценщиками и органами оценки по безопасности, предоставляемой ОО, и области применения оценки. Круг лиц, заинтересованных в ЗБ, может также включать ответственных за управление, маркетинг, продажу, инсталляцию, конфигурирование, функционирование и применение ОО. ЗБ включает следующие разделы:

Введение

Содержит маркировку ЗБ (и ОО, для которого оно разработано), аннотацию ЗБ и утверждение о соответствии ОК. Аннотация предназначена для потенциального пользователя ОО и пригодна для включения в перечни оцененных продуктов. Утверждение о соответствии ОК устанавливает некоторое оцениваемое утверждение о соответствии ОО Общим критериям и может включать ссылки на профили защиты или оценочный уровень доверия. При необходимости может быть указан минимальный уровень стойкости функций безопасности.

Описание ОО.

Устанавливает контекст оценки. Способствует пониманию требований безопасности ОО и дает представление о типе ОО, его предполагаемом применении и основных характеристиках безопасности.

Среда безопасности.

Как и для ПЗ, содержит описание угроз, политики безопасности организации, которой ОО должен соответствовать, а также аспектов безопасности среды, в которой предполагается применение ОО (предположений).

Цели безопасности.

Включают цели безопасности как для ОО, так и для поддерживающей его среды. Эти цели направлены на противостояние идентифицированным угрозам и соответствуют политике безопасности организации и предположениям.

Требования безопасности ИТ.

Приводятся требования безопасности ИТ ОО, включая конкретизированные функциональные требования и требования доверия. Там, где это необходимо, указываются требования безопасности для среды ИТ. Требования, выражаемые

ссылкой на ПЗ, не обязательно повторяются в ЗБ. При необходимости также следует указать минимальный уровень стойкости функций безопасности.

Утверждения о соответствии ПЗ.

Если в ЗБ заявлено о соответствии ОО требованиям одного или нескольких ПЗ, то требуются пояснения, мотивировка и прочие вспомогательные материалы. Здесь содержится ссылка на ПЗ, описание уточнений ПЗ и описание дополнений к ПЗ.

Краткая спецификация ОО.

Обеспечивает высокоуровневое определение функций безопасности, заявленных для выполнения функциональных требований, и мер безопасности, предпринимаемых для выполнения требований доверия. При необходимости для отдельных функций безопасности может быть заявлена стойкость функций.

Обоснование.

Демонстрирует, что ЗБ содержит полную и взаимосвязанную совокупность пригодных для использования и эффективных контрмер.

Оценка.

Оценкой называется проверка продукта или системы ИТ по определенным критериям. Оценка по ОК использует ОК как основу для оценивания характеристик безопасности ИТ. Оценки по единому стандарту повышают сопоставимость итоговых результатов оценок. Чтобы далее повышать сопоставимость результатов оценок, они должны быть выполнены в рамках полномочной системы оценки, в которой установлены стандарты и постоянно контролируется качество оценок. Такие системы существуют в настоящее время во многих странах.

Определены различные стадии оценки, соответствующие основным уровням представления ОО.

– оценка ПЗ – выполняемая по критериям оценки для ПЗ (из части 3 ОК);

– оценка ЗБ – выполняемая по критериям оценки для ЗБ (из части 3 ОК);

– оценка ОО – выполняемая по критериям оценки из части 3 ОК с использованием оцененного ЗБ в качестве основы;

– поддержание доверия – выполняемое в соответствии со схемой, основанной на требованиях из части 3 ОК.

Тестирование, проверка проекта и проверка реализации вносят значительный вклад в снижение риска наличия нежелательного поведения ОО. ОК представляют структуру проведения экспертного анализа (оценки) в указанных областях.

Профили защиты Общих критериев.

Ранние версии ОК содержали примеры ПЗ, которые были идентифицированы в исходных критериях, и предложения по процедурам создания и управления реестром одобренных ПЗ. Сейчас реестр ПЗ в ОК не рассматривается. Имеется в виду, что будет создана система взаимосвязанных национальных реестров. ПЗ могут быть определены как разработчиками при формулировании спецификаций безопасности для ОО, так и сообществами пользователей.

Примеры ПЗ

Существенные усилия для разработки профилей защиты уже приложены правительственными, промышленными и коммерческими организациями. Некоторые примеры разработок, которые выполнены в настоящее время:

- базовый коммерческий профиль защиты;
- профили, отражающие требования классов С2 и В1 «Оранжевой книги»;
- профиль управления доступом, основанного на ролях;
- профили для смарт–карт;
- профиль для реляционных баз данных;
- профили межсетевых экранов для пакетных фильтров и шлюзов приложений.

Расширяемость ОК.

Допускается расширение ОК, для чего возможно определение функциональных требований и требований доверия, не содержащихся в ОК. Расширенные функциональные требования и требования доверия должны соответствовать критериям расширяемости ОК. Рекомендуется, чтобы компоненты, не определенные в ОК, тщательно анализировались перед введением таких расширений, поскольку

использование расширенных требований может потребовать предварительного одобрения органа оценки.

Тема 2.5 Рекомендации X.800 для распределенных систем

1 Рекомендации X.800 для распределенных систем

Рекомендации X.800 определяют функции (сервисы) безопасности, характерные для распределенных систем, уровни эталонной семиуровневой модели OSI, на которых могут быть реализованы функции безопасности, используемые механизмы безопасности, а также администрирование средств безопасности.

Функции (сервисы) безопасности включают:

- аутентификацию;
- управление доступом;
- конфиденциальность данных;
- целостность данных;
- неотказуемость.

В таблице 1 указаны уровни эталонной модели OSI, на которых могут быть реализованы функции безопасности.

* – уровень эталонной семиуровневой модели OSI, на котором могут быть реализованы функции безопасности.

Для реализации функций безопасности могут использоваться следующие механизмы и их комбинации (см. таблицу 3).

Выделяют следующие сервисы безопасности и исполняемые ими роли:

1) Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

Таблица 1 – Рекомендации X.800. Функции и механизмы безопасности

Функции безопасности	**Уровень***						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1.Аутентификация			+	+			+
2.Управление доступом			+	+			+
3.Конфиденциальность соединения	+	+	+	+		+	+
4.Конфиденциальность вне соединения		+	+	+		+	+
5.Избирательная конфиденциальность						+	+
6.Конфиденциальность трафика	+		+				+
7.Целостность с восстановлением				+			+
8.Целостность без восстановления			+	+			+
9.Избирательная целостность							+
10.Целостность вне соединения			+	+			+
11.Неотказуемость							+

Таблица 2 – Механизмы и их комбинации

	Механизмы							
Функции безопасности	**Шифрование**	**Электронная подпись**	**Управление доступом**	**Контроль целостности данных**	**Аутентификация**	**Дополнение трафика**	**Управление маршрутизацией**	**Нотаризация**
1.Аутентификация партнеров	+	+			+			
2.Аутентификация источника	+	+						
3.Управление доступом			+					
4.Конфиденциальность	+						+	
5.Избирательная конфиденциальность	+							
6.Конфиденциальность трафика	+					+	+	
7.Целостность соединения	+			+				
8.Целостность вне соединения	+	+		+				
9.Неотказуемость		+		+				+

2) Управление доступом. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

3) Конфиденциальность данных. Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем

конфиденциальность трафика (это защита информации, которую можно получить, анализируя сетевые потоки данных).

4) Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

5) Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.

2 Шифрование

Шифрование подразделяется на симметричное (с секретным ключом, когда знание ключа шифрования влечет знание ключа расшифровки) и асимметричное (с открытым ключом, когда знание ключа шифрования не позволяет узнать ключ расшифровки).

Различают также обратимое и необратимое шифрование. Последнее может использоваться для вычисления криптографических контрольных сумм.

Электронная (цифровая) подпись.

Механизм электронной подписи включает в себя две процедуры:

1) Выработку подписи.

2) Проверку подписанной порции данных. Процедура выработки подписи использует информацию, известную только лицу, подписывающему порцию данных. Процедура проверки подписи является общедоступной, она не должна позволять найти секретный ключ подписывающего.

3 Механизмы управления доступом

1) Базы данных управления доступом. В такой базе, поддерживаемой централизованно или на оконечных системах, могут храниться списки управления доступом или структуры аналогичного назначения.

2) Пароли или иная аутентификационная информация.

3) Токены, билеты или иные удостоверения, предъявление которых свидетельствует о наличии прав доступа.

4) Метки безопасности, ассоциированные с субъектами и объектами доступа.

5) Время запрашиваемого доступа.

6) Маршрут запрашиваемого доступа.

7) Длительность запрашиваемого доступа.

4 Механизмы контроля целостности данных

Различают два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации.

Процедура контроля целостности отдельного сообщения (поля) базируется на использовании контрольных сумм. Данный механизм не защищает от дублирования сообщений.

Для проверки целостности потока сообщений (то есть для защиты от хищения, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание (когда результат шифрования очередного сообщения зависит от предыдущего) или иные аналогичные приемы.

При общении в режиме без установления соединения использование временных штампов может обеспечить ограниченную форму защиты от дублирования сообщений.

5 Механизмы аутентификации и дополнения трафика

Аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик.

Механизмы дополнения трафика эффективны только в сочетании со средствами обеспечения конфиденциальности, поскольку в противном случае злоумышленнику будет очевиден фиктивный характер дополнительных сообщений.

6 Механизмы управления маршрутизацией и нотаризации

Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными.

Механизм нотаризации служит для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателя. Заверение обеспечивается надежной третьей стороной, которая обладает достаточной информацией, чтобы ее заверениям можно было доверять. Обычно нотаризация опирается на механизм электронной подписи.

7 Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы функций и механизмов безопасности, а также сбор и анализ информации об их функционировании. Администрирование средств безопасности в распределенной среде имеет много особенностей по сравнению с централизованными системами. Так, например, обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов и могут включать:

1) Управление ключами (генерация и распределение).

2) Управление шифрованием (установка и синхронизация криптографических параметров). Администрирование механизмов электронной подписи.

3) Управление целостностью, если оно обеспечивается криптографическими средствами.

4) Администрирование управления доступом (распределение паролей, списков доступа и т.п.).

5) Управление аутентификацией (распределение информации, необходимой для управления - паролей, ключей и т.п.).

6) Управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений - частоту отправки, размер и т.п.).

Характеристики могут варьироваться по заданному закону в зависимости от даты и времени.

7) Управление маршрутизацией (выделение надежных путей).

8) Управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Тема 2.6 Система стандартов в области защиты информации

1 Система стандартов по защите информации

Система стандартов по защите информации (ССЗИ) – совокупность взаимосвязанных стандартов, устанавливающих характеристики продукции, правила осуществления и характеристики процессов, выполнения работ или оказания услуг в области защиты информации.

Национальные стандарты (ГОСТы) в общем случае являются рекомендательными. Однако в ряде случаев обязательность следования стандартам и спецификациям закреплена законодательно. В соответствии со ст.6 ФЗ №162 «О стандартизации в Российской Федерации» в том случае, если речь идет о стандартизации в отношении оборонной продукции (товаров, работ, услуг) по государственному оборонному заказу, продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции, сведения о которой составляют государственную тайну, продукции, для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии, а также в отношении процессов и иных объектов стандартизации, связанных с такой продукцией, стандарты являются обязательными к применению.

Основополагающим стандартом РФ в области защиты информации (не-криптографическими методами) является ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения».

Целью создания ССЗИ является достижение рациональной упорядоченности организации и содержания работ в области ЗИ, повышение эффективности ЗИ на основе установления общих правил и характеристик для их многократного использования, а также повышение эффективности работ по стандартизации за счет упорядочения структуры системы стандартов, процесса разработки стандартов, учета взаимосвязи стандартов различных систем.

Основными задачами по формированию и развитию ССЗИ являются:

- установление основополагающих принципов построения, требований к составу и содержанию системы документов в области ЗИ;
- обеспечение единства терминологии в области ЗИ;
- упорядочение объектов и аспектов стандартизации в области ЗИ;
- обеспечение единства организационных и методических подходов к проведению работ по ЗИ;
- установление системы требований по ЗИ, предъявляемых к различным видам ОЗИ, и методов контроля выполнения этих требований;
- установление общих технических требований к СЗИ и СКЭЗИ, методам их испытаний;
- установление общих требований к услугам по ЗИ;
- установление требований к методам и методикам испытаний и оценки качества СЗИ и СКЭЗИ, к методам и методикам измерений в процессе контроля эффективности мероприятий по ЗИ;
- установление требований к метрологическому, информационному и другим видам обеспечения ЗИ.

Система стандартов по защите информации включает следующие виды документов в области стандартизации по ЗИ, используемых на территории Российской Федерации:

- национальные стандарты Российской Федерации, в том числе ограниченного распространения, государственные военные стандарты, национальные стандарты, оформленные на основе аутентичных переводов международных стандартов (гармонизированные стандарты);
- межгосударственные стандарты;
- правила стандартизации, нормы и рекомендации в области стандартизации;
- общероссийские классификаторы технико-экономической и социальной информации;
- стандарты организаций;
- предварительные национальные стандарты.

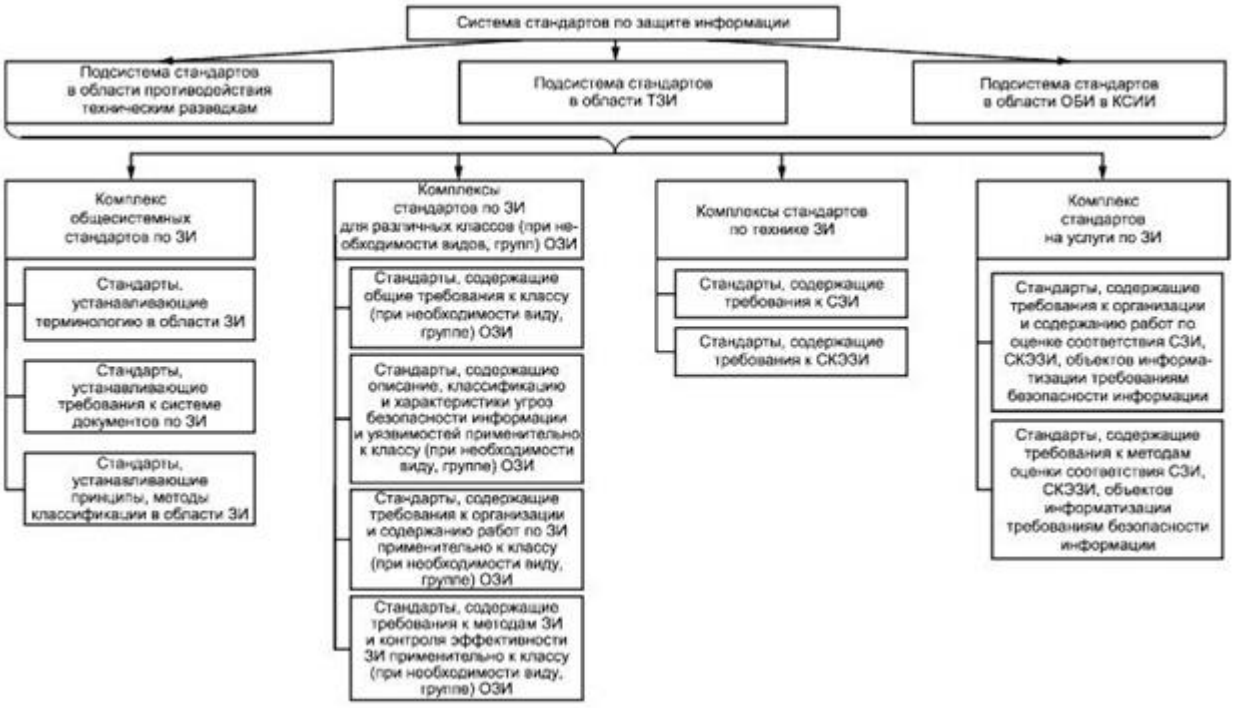

Рисунок 1 – Структура системы стандартов по защите информации

Сокращения на рисунке:

- ЗИ – защита информации;
- ОБИ в КСИИ – обеспечение безопасности информации в ключевых системах информационной инфраструктуры;
- ОЗИ – объект защиты информации;
- СЗИ – средство защиты информации;
- СКЭЗИ – средство контроля эффективности защиты информации;
- ТЗИ – техническая защита информации.