МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Семиноженко Д. В. ИБО-ФМ-19

Область применения

Данная часть ИСО/МЭК 15408 определяет требования доверия ИСО/МЭК 15408 и включает оценочные уровни доверия (ОУД), определяющие шкалу для измерения доверия для ОО-компонентов, составные пакеты доверия (СоПД), определяющие шкалу для измерения доверия для составных ОО, отдельные компоненты доверия, из которых составлены уровни и пакеты доверия, а также критерии для оценки ПЗ и ЗБ.

Основные принципы

Основные принципы ИСО/МЭК 15408 состоят в том, что следует четко сформулировать угрозы безопасности и положения политики безопасности организации, а достаточность предложенных мер безопасности должна быть продемонстрирована. Более того, следует принять меры по уменьшению вероятности наличия уязвимостей, возможности их проявления (т.е. преднамеренного использования или непреднамеренной активизации), а также степени ущерба, который может явиться следствием проявления уязвимости. Дополнительно следует предпринять меры для облегчения последующей идентификации уязвимостей, а также по их устранению, ослаблению и/или оповещению об их использовании или активизации.

Подход к доверию

Основная концепция ИСО/МЭК 15408 - обеспечение доверия, основанное на оценке (активном исследовании) продукта ИТ, который должен соответствовать определенным критериям безопасности. Оценка была традиционным способом обеспечения доверия и являлась основой предшествующих критериев оценки. Для согласования с существующими подходами в ИСО/МЭК 15408 принят тот же самый основной принцип. В ИСО/МЭК 15408 предполагается, что проверку правильности документации и разработанного продукта ИТ будут проводить опытные оценщики, уделяя особое внимание области, глубине и строгости оценки.

Основные принципы ИСО/МЭК 15408 содержат утверждение, что большее доверие является результатом приложения больших усилий при оценке, и что цель состоит в применении минимальных усилий, требуемых для обеспечения необходимого уровня доверия. Повышение уровня усилий может быть основано на:

- области охвата, т.е. увеличении рассматриваемой части продукта ИТ;
- глубине, т.е. детализации рассматриваемых проектных материалов и реализации;
- строгости, т.е. применении более структурированного и формального подхода.

Причины уязвимостей

Уязвимости могут возникать из-за недостатков:

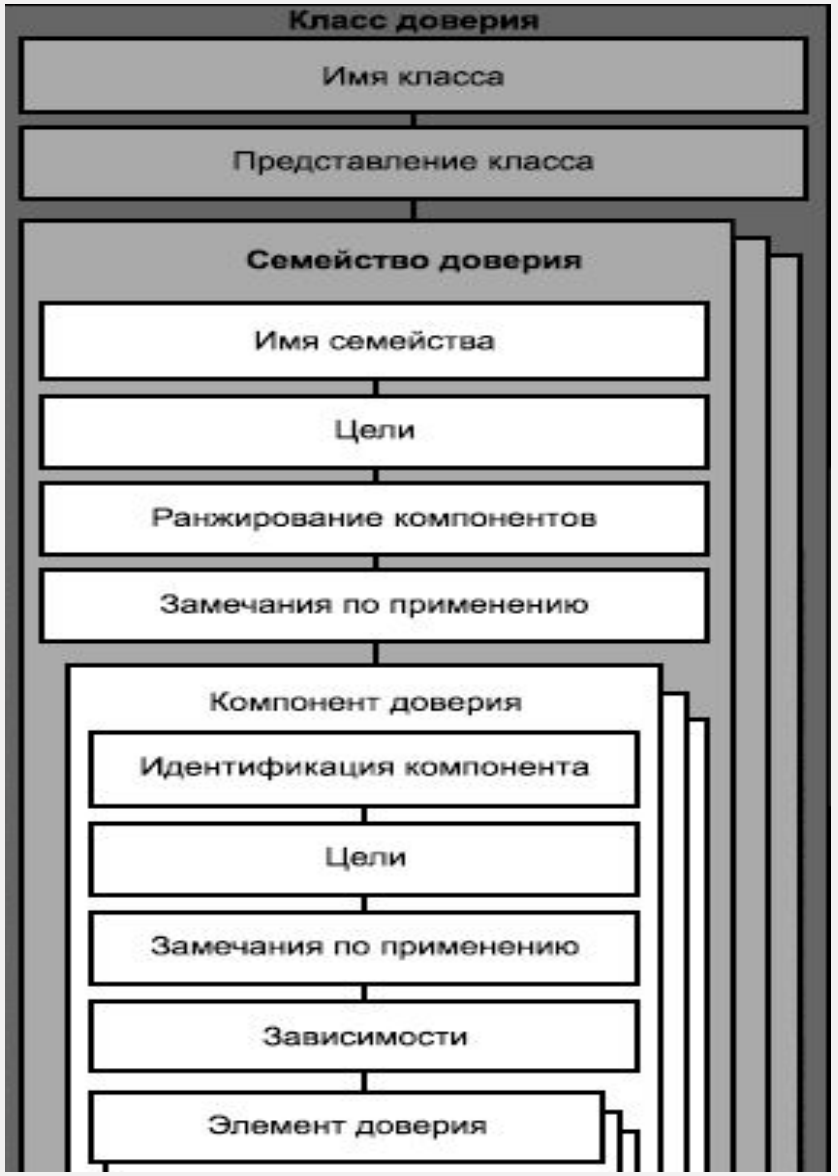
a) требований, т.е. продукт ИТ может обладать требуемыми от него функциями и свойствами, но все же содержать уязвимости, которые делают его непригодным или неэффективным в части безопасности;

b) проектирования, т.е. продукт ИТ не отвечает спецификации, и/или уязвимости являются следствием некачественных стандартов проектирования или неправильных проектных решений;

c) эксплуатации, т.е. продукт ИТ разработан в полном соответствии с корректной спецификацией, но уязвимости возникают как результат неадекватного управления при эксплуатации.

Структура классов, семейств и компонентов доверия к безопасности

Структура компонента доверия



Иерархическая структура представления требований доверия: класс-семейство-компонент-элемент

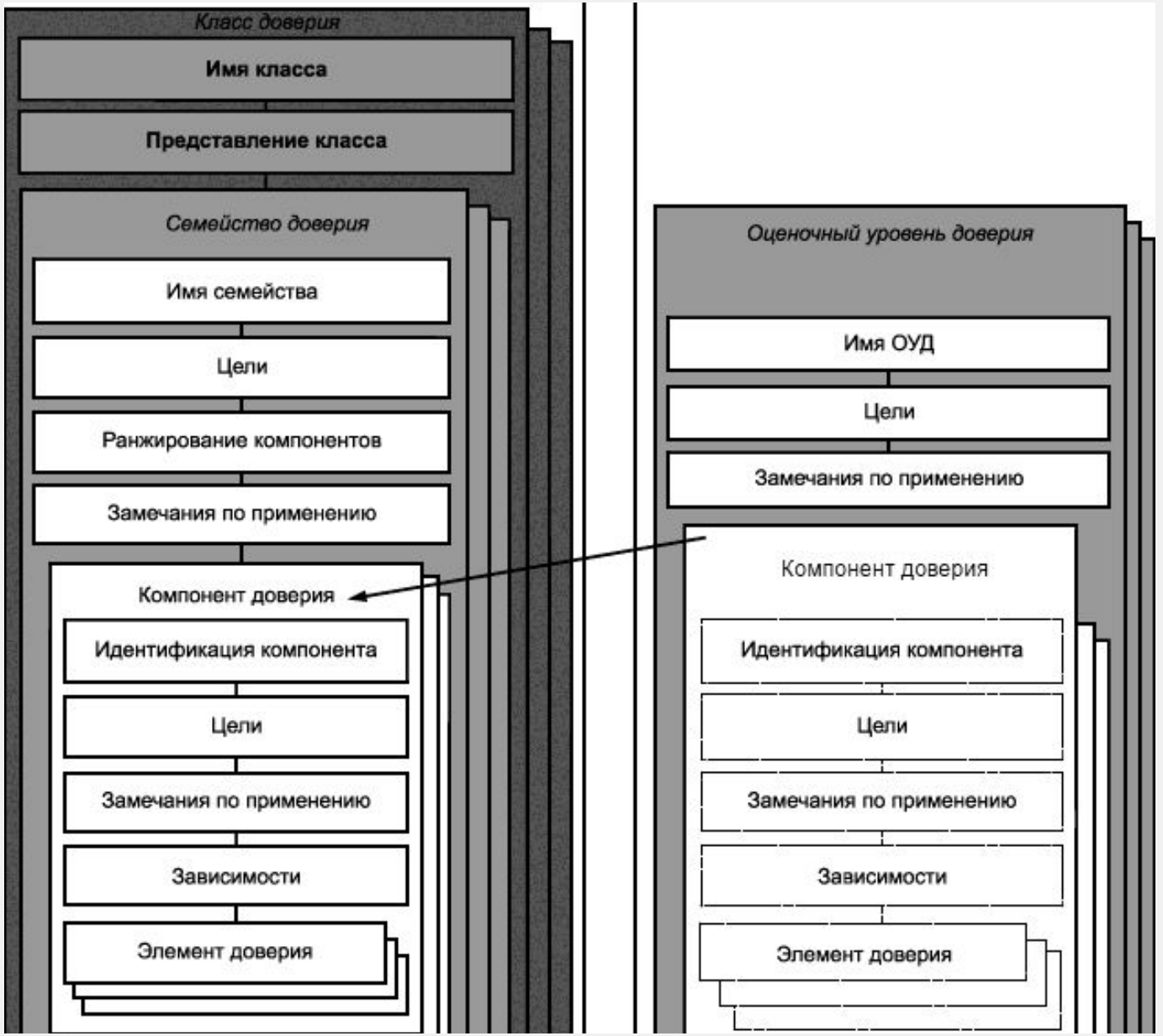
Структура ОУД

Для каждого ОУД выбран набор компонентов требований доверия. Более высокий уровень доверия, чем предоставляемый конкретным ОУД, может быть достигнут:

a) включением дополнительных компонентов требований доверия из других семейств доверия или
b) заменой компонента требований доверия иерархичным компонентом из этого же семейства требований доверия.

Взаимосвязь между требованиям и и уровнями доверия

Компоненты доверия состоят из элементов, но на последние в отдельности не могут ссылаться оценочные уровни доверия. Стрелка на рисунке отображает ссылку в ОУД на компонент требований доверия внутри класса, в котором он определен.



Структура СоПД

Структура СоПД аналогична структуре ОУД. Ключевое различие двух структур состоит в типе ОО, к которым они применяются; ОУД применяется к ОО-компонентам, а СоПД - ко всему составному ОО в целом.

Обзор оценочных уровней доверия

Класс доверия	Семейство доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Разработка	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	3	**4**	**5**	5	6
	ADV_IMP				**1**	1	2	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	3	**4**	**5**	**6**
Руководства	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_CMC	**1**	**2**	3	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	3	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	3	3

Столбцы таблицы представляют иерархически упорядоченный набор ОУД, а строки - семейства доверия. Каждый номер в образованной ими матрице идентифицирует конкретный компонент доверия, применяемый в данном случае.

Обзор оценочных уровней доверия (ОУД)

Класс доверия	Семейство доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Оценка задания по безопасности	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Тестирование	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	**2**	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	2	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Оценка уязвимостей	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Уровень доверия 1

Класс доверия	Компоненты доверия
ADV: Разработка	ADV_FSP.1 Базовая функциональная спецификация
AGD: Руководства	AGD_OPE.1 Руководство пользователя по эксплуатации
	AGD_PRE.1 Подготовительные процедуры
ALC: Поддержка жизненного цикла	ALC_CMC.1 Маркировка ОО
	ALC_CMS.1 Охват УК объекта оценки
ASE: Оценка задания по безопасности	ASE_CCL.1 Утверждения о соответствии
	ASE_ECD.1 Определение расширенных компонентов
	ASE_INT.1 Введение ЗБ
	ASE_OBJ.1 Цели безопасности для среды функционирования
	ASE_REQ.1 Установленные требования безопасности
	ASE_TSS.1 Краткая спецификация ОО
ATE: Тестирование	ATE_IND.1 Независимое тестирование на соответствие
AVA: Оценка уязвимостей	AVA_VAN.1 Обзор уязвимостей

Уровень доверия 2

Класс доверия	Компоненты доверия
ADV: Разработка	ADV_ARC.1 Описание архитектуры безопасности
	ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации
	ADV_TDS.1 Базовый проект
AGD: Руководства	AGD_OPE.1 Руководство пользователя по эксплуатации
	AGD_PRE.1 Подготовительные процедуры
ALC: Поддержка жизненного цикла	ALC_CMC.2 Использование системы УК
	ALC_CMS.2 Охват УК частей ОО
	ALC_DEL.1 Процедуры поставки
ASE: Оценка задания по безопасности	ASE_CCL.1 Утверждения о соответствии
	ASE_ECD.1 Определение расширенных компонентов
	ASE_INT.1 Введение ЗБ
	ASE_OBJ.2 Цели безопасности
	ASE_REQ.2 Производные требования безопасности
	ASE_SPD.1 Определение проблемы безопасности
	ASE_TSS.1 Краткая спецификация ОО
ATE: Тестирование	ATE_COV.1 Свидетельство покрытия
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_VAN.2 Анализ уязвимостей

Уровень доверия 3

Класс доверия	Компоненты доверия
ADV: Разработка	ADV_ARC.1 Описание архитектуры безопасности
	ADV_FSP.3 Функциональная спецификация с полной аннотацией
	ADV_TDS.2 Архитектурный проект
AGD: Руководства	AGD_OPE.1 Руководство пользователя по эксплуатации
	AGD_PRE.1 Подготовительные процедуры
ALC: Поддержка жизненного цикла	ALC_CMC.3 Средства управления авторизацией
	ALC_CMS.3 Охват УК представления реализации
	ALC_DEL.1 Процедуры поставки
	ALC_DVS.1 Идентификация мер безопасности
	ALC_LCD.1 Определенная разработчиком модель жизненного цикла
ASE: Оценка задания по безопасности	ASE_CCL.1 Утверждения о соответствии
	ASE_ECD.1 Определение расширенных компонентов
	ASE_INT.1 Введение ЗБ
	ASE_OBJ.2 Цели безопасности
	ASE_REQ.2 Производные требования безопасности
	ASE_SPD.1 Определение проблемы безопасности
	ASE_TSS.1 Краткая спецификация ОО
ATE: Тестирование	ATE_COV.2 Анализ покрытия
	ATE_DPT.1 Тестирование: базовый проект
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_VAN.2 Анализ уязвимостей

Уровень доверия 4

Класс доверия	Компоненты доверия
ADV: Разработка	ADV_ARC.1 Описание архитектуры безопасности
	ADV_FSP.4 Полная функциональная спецификация
	ADV_IMP.1 Представление реализации ФБО
	ADV_TDS.3 Базовый модульный проект
AGD: Руководства	AGD_OPE.1 Руководство пользователя по эксплуатации
	AGD_PRE.1 Подготовительные процедуры
ALC: Поддержка жизненного цикла	ALC_CMC.4 Поддержка производства, процедуры приемки и автоматизации
	ALC_CMS.4 Охват УК отслеживания проблем
	ALC_DEL.1 Процедуры поставки
	ALC_DVS.1 Идентификация мер безопасности
	ALC_LCD.1 Определенная разработчиком модель жизненного цикла
	ALC_TAT.1 Полностью определенные инструментальные средства разработки
ASE: Оценка задания по безопасности	ASE_CCL.1 Утверждения о соответствии
	ASE_ECD.1 Определение расширенных компонентов
	ASE_INT.1 Введение ЗБ
	ASE_OBJ.2 Цели безопасности
	ASE_REQ.2 Производные требования безопасности
	ASE_SPD.1 Определение проблемы безопасности
	ASE_TSS.1 Краткая спецификация ОО
ATE: Тестирование	ATE_COV.2 Анализ покрытия
	ATE_DPT.2 Тестирование: модули обеспечения безопасности
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_VAN.3 Сосредоточенный анализ уязвимостей

Уровень доверия 5

Класс доверия	Компоненты доверия
ADV: Разработка	ADV_ARC.1 Описание архитектуры безопасности
	ADV_FSP.5 Полная полуформальная спецификация с дополнительной информацией об ошибках
	ADV_IMP.1 Представление реализации ФБО
	ADV_INT.2 Полностью определенная внутренняя структура
	ADV_TDS.4 Полуформальный модульный проект
AGD: Руководства	AGD_OPE.1 Руководство пользователя по эксплуатации
	AGD_PRE.1 Подготовительные процедуры
ALC: Поддержка жизненного цикла	ALC_CMC.4 Поддержка производства, процедуры приемки и автоматизации
	ALC_CMS.5 Охват УК инструментальных средств разработки
	ALC_DEL.1 Процедуры поставки
	ALC_DVS.1 Идентификация мер безопасности
	ALC_LCD.1 Определенная разработчиком модель жизненного цикла
	ALC_TAT.2 Соответствие стандартам реализации
ASE: Оценка задания по безопасности	ASE_CCL.1 Утверждения о соответствии
	ASE_ECD.1 Определение расширенных компонентов
	ASE_INT.1 Введение ЗБ
	ASE_OBJ.2 Цели безопасности
	ASE_REQ.2 Производные требования безопасности
	ASE_SPD.1 Определение проблемы безопасности
	ASE_TSS.1 Краткая спецификация ОО
ATE: Тестирование	ATE_COV.2 Анализ покрытия
	ATE_DPT.3 Тестирование: модульный проект
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_VAN.4 Методический анализ уязвимостей

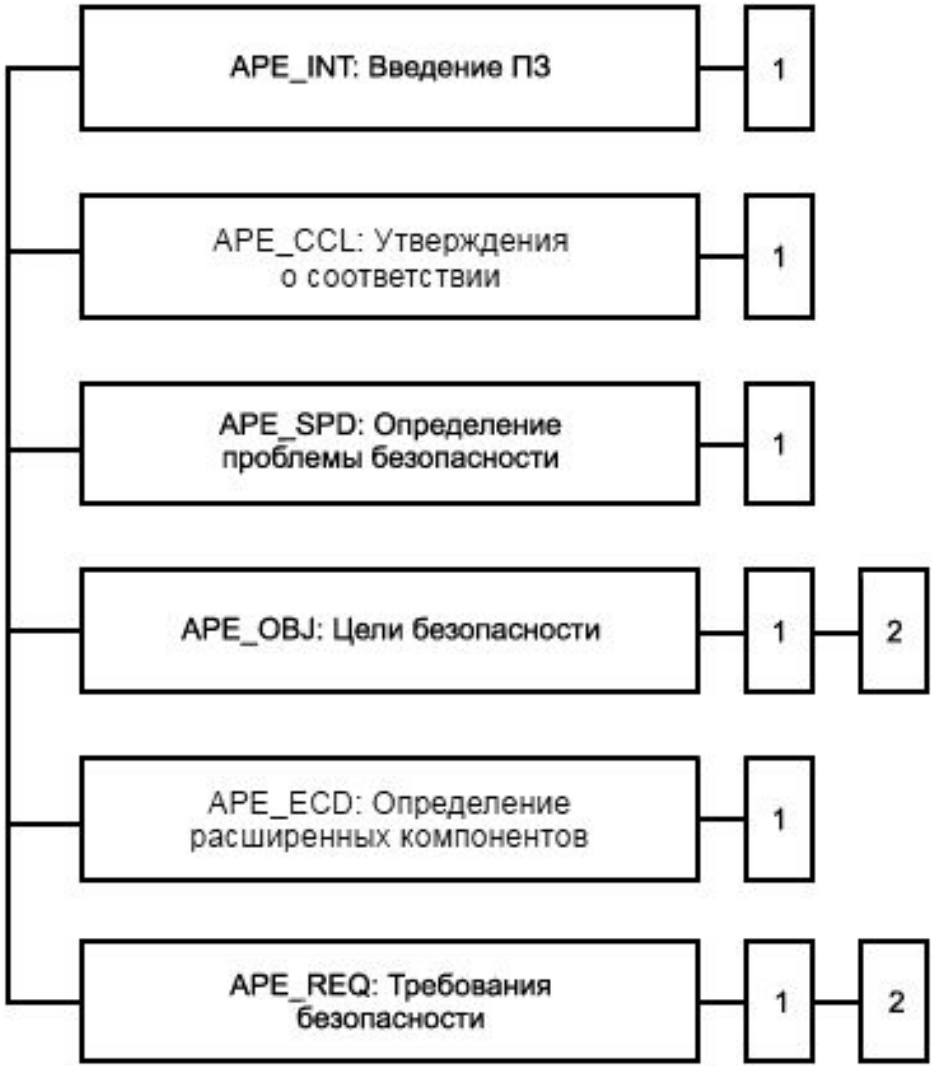
Уровень доверия 6

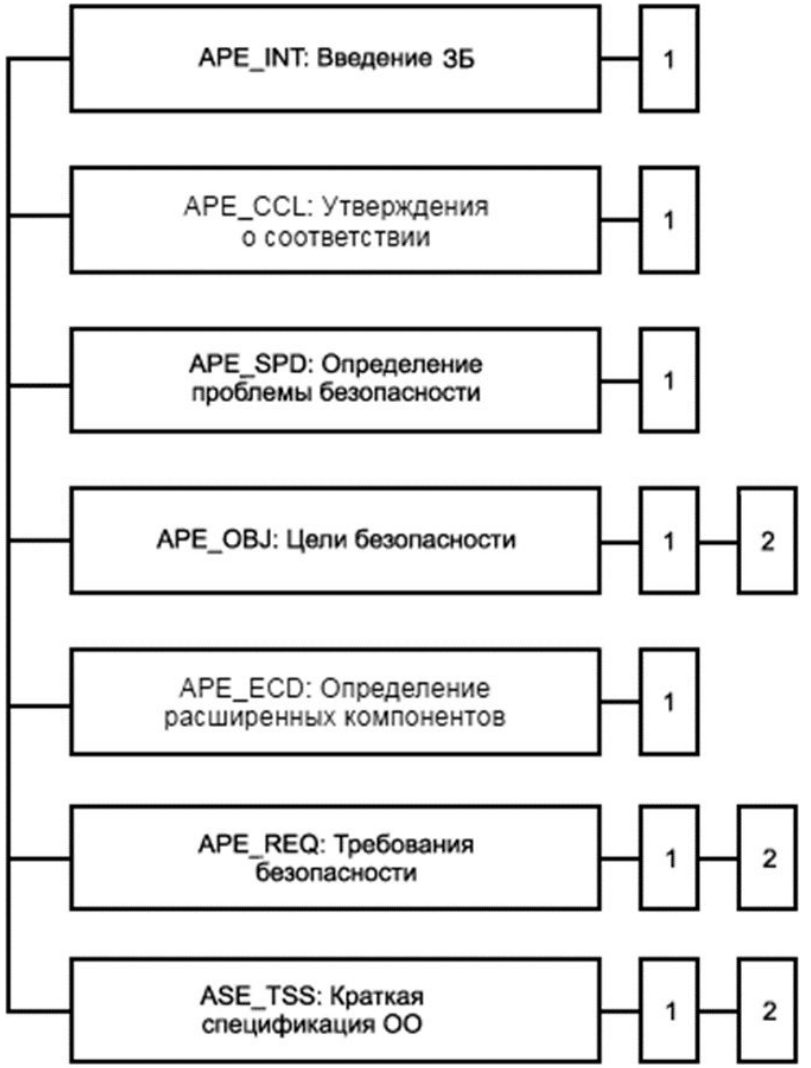
Класс доверия	Компоненты доверия
ADV: Разработка	ADV_ARC.1 Описание архитектуры безопасности
	ADV_FSP.5 Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках
	ADV_IMP.2 Полное прослеживание представления реализации ФБО
	ADV_INT.3 Минимальная сложность внутренней структуры системы
	ADV_SPM.1 Формальная модель политики безопасности ОО
	ADV_TDS.5 Полный полуформальный модульный проект
AGD: Руководства	AGD_OPE.1 Руководство пользователя по эксплуатации
	AGD_PRE.1 Подготовительные процедуры
ALC: Поддержка жизненного цикла	ALC_CMC.5 Расширенная поддержка
	ALC_CMS.5 Охват УК инструментальных средств разработки
	ALC_DEL.1 Процедуры поставки
	ALC_DVS.2 Достаточность мер безопасности
	ALC_LCD.1 Определенная разработчиком модель жизненного цикла
	ALC_TAT.3 Соответствие всех частей ОО стандартам реализации
ASE: Оценка задания по безопасности	ASE_CCL.1 Утверждения о соответствии
	ASE_ECD.1 Определение расширенных компонентов
	ASE_INT.1 Введение ЗБ
	ASE_OBJ.2 Цели безопасности
	ASE_REQ.2 Производные требования безопасности
	ASE_SPD.1 Определение проблемы безопасности
	ASE_TSS.1 Краткая спецификация ОО
ATE: Тестирование	ATE_COV.3 Строгий анализ покрытия
	ATE_DPT.3 Тестирование: модульный проект
	ATE_FUN.2 Упорядоченное функциональное тестирование
	ATE_IND.3 Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_VAN.5 Усиленный методический анализ уязвимостей

Уровень доверия 7

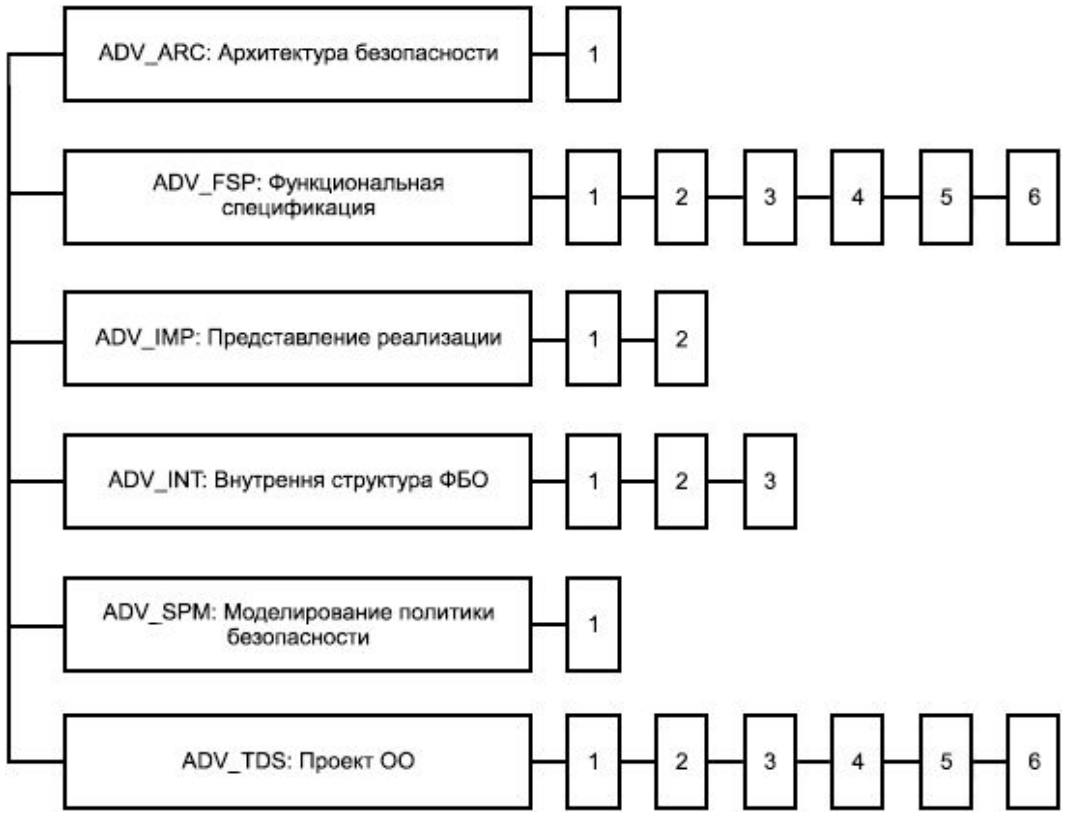
Класс доверия	Компоненты доверия
ADV: Разработка	ADV_ARC.1 Описание архитектуры безопасности
	ADV_FSP.6 Полная полуформальная функциональная спецификация с дополнительной формальной спецификацией
	ADV_IMP.2 Полное прослеживание представления реализации ФБО
	ADV_INT.3 Минимальная сложность внутренней структуры системы
	ADV_SPM.1 Формальная модель политики безопасности ОО
	ADV_TDS.6 Полный полуформальный модульный проект с формальным представлением проекта верхнего уровня
AGD: Руководства	AGD_OPE.1 Руководство пользователя по эксплуатации
	AGD_PRE.1 Подготовительные процедуры
ALC: Поддержка жизненного цикла	ALC_CMC.5 Расширенная поддержка
	ALC_CMS.5 Охват УК инструментальных средств разработки
	ALC_DEL.1 Процедуры поставки
	ALC_DVS.2 Достаточность мер безопасности
	ALC_LCD.2 Измеримая модель жизненного цикла
	ALC_TAT.3 Соответствие всех частей ОО стандартам реализации
ASE: Оценка задания по безопасности	ASE_CCL.1 Утверждения о соответствии
	ASE_ECD.1 Определение расширенных компонентов
	ASE_INT.1 Введение ЗБ
	ASE_OBJ.2 Цели безопасности
	ASE_REQ.2 Производные требования безопасности
	ASE_SPD.1 Определение проблемы безопасности
	ASE_TSS.1 Краткая спецификация ОО
ATE: Тестирование	ATE_COV.3 Строгий анализ покрытия
	ATE_DPT.4 Тестирование: представление реализации
	ATE_FUN.2 Упорядоченное функциональное тестирование
	ATE_IND.3 Полное независимое тестирование
AVA: Оценка уязвимостей	AVA_VAN.5 Усиленный методический анализ уязвимостей

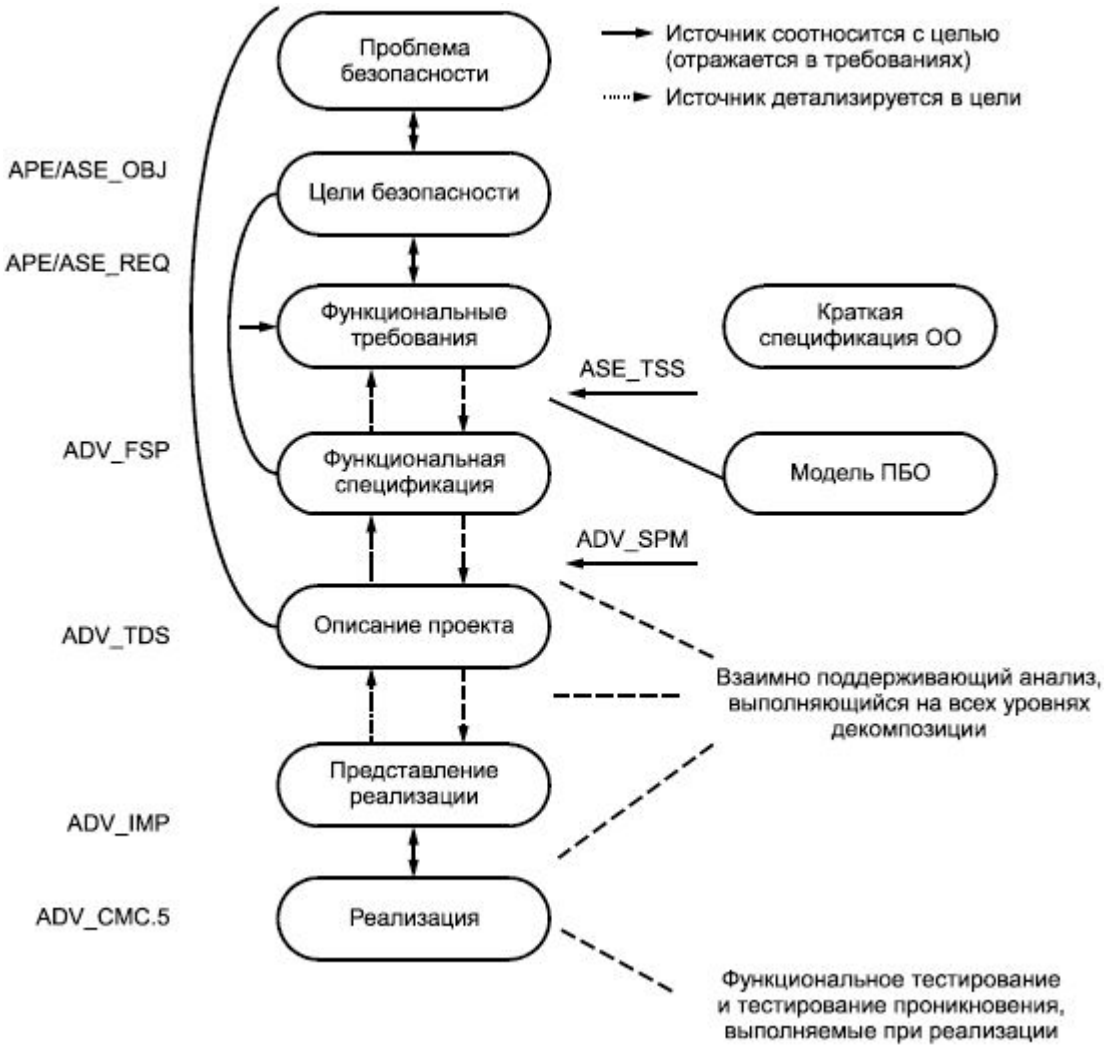
Семейства класса APE, ASE и иерархия компонентов в семействах



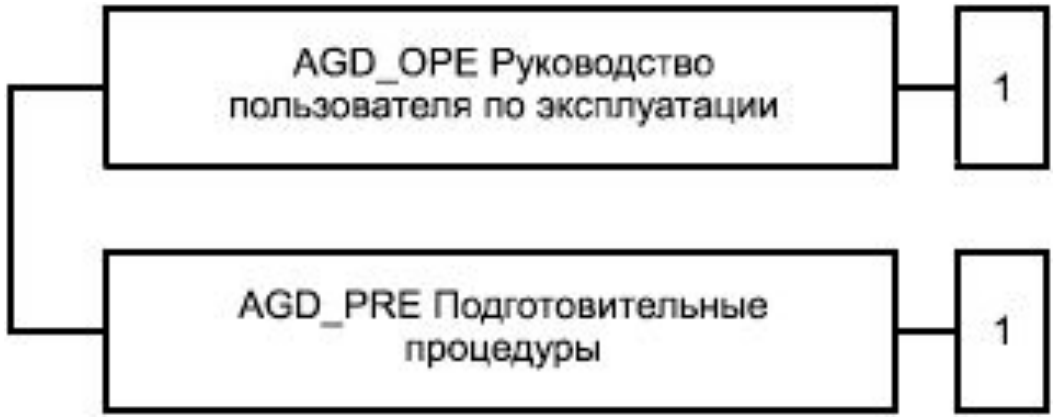


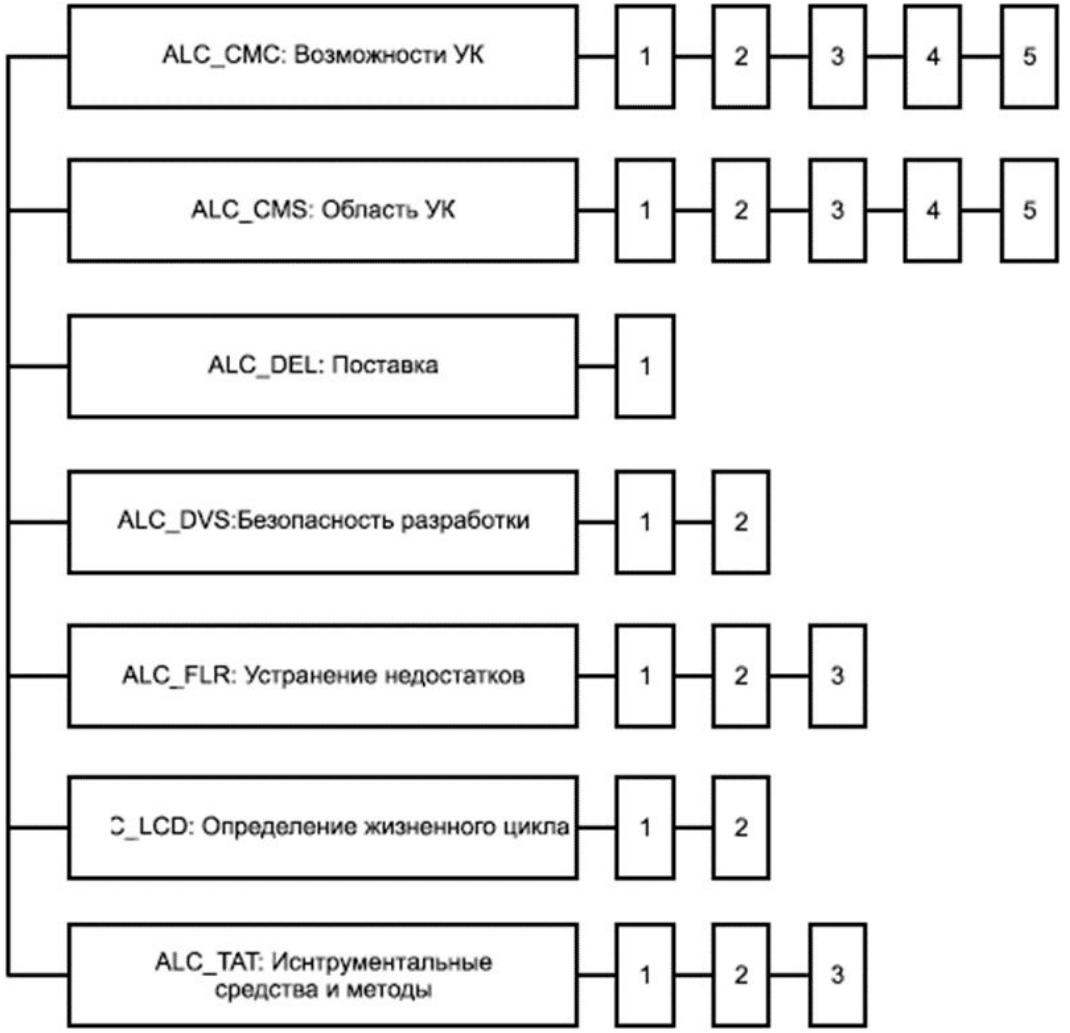
Семейства класса ADV и иерархия компонентов в семействах, их взаимодействие





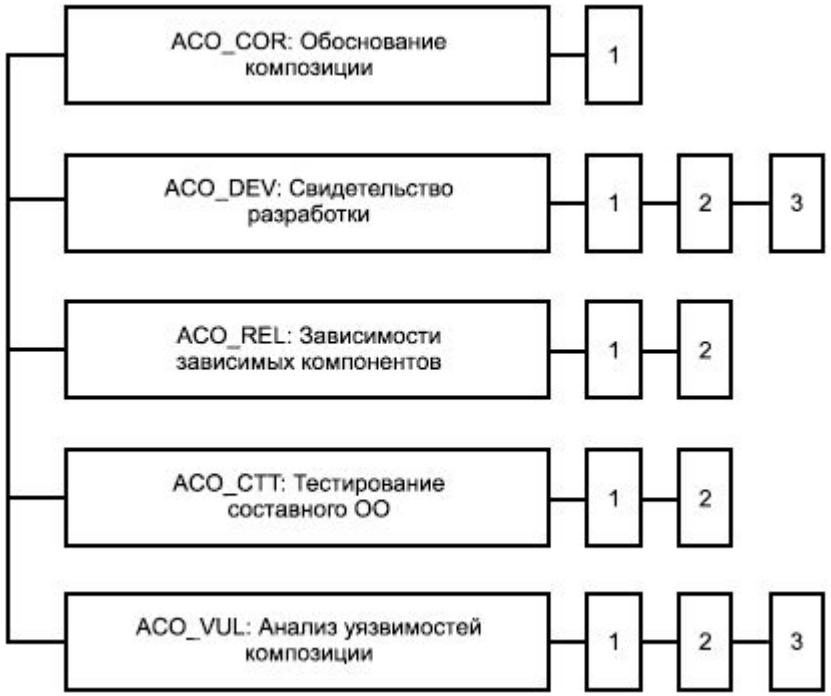
Семейства класса AGD, ALC и иерархия компонентов в семействах

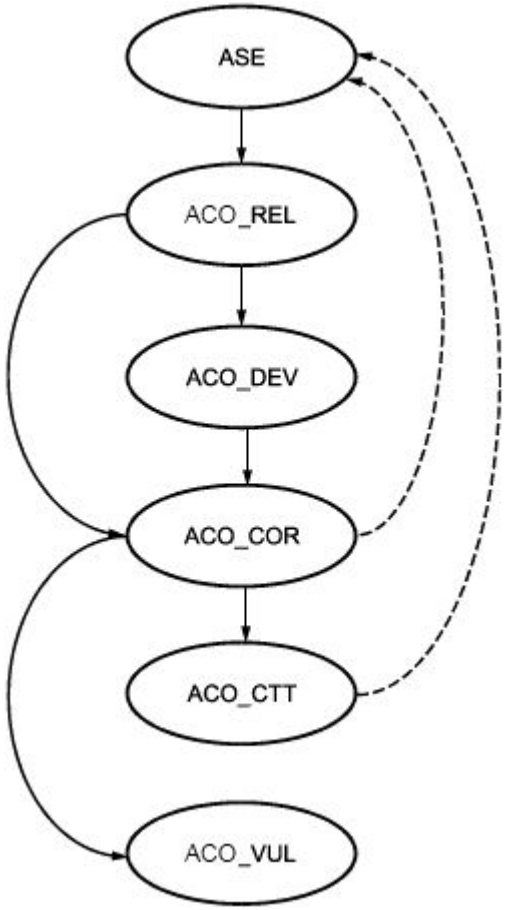




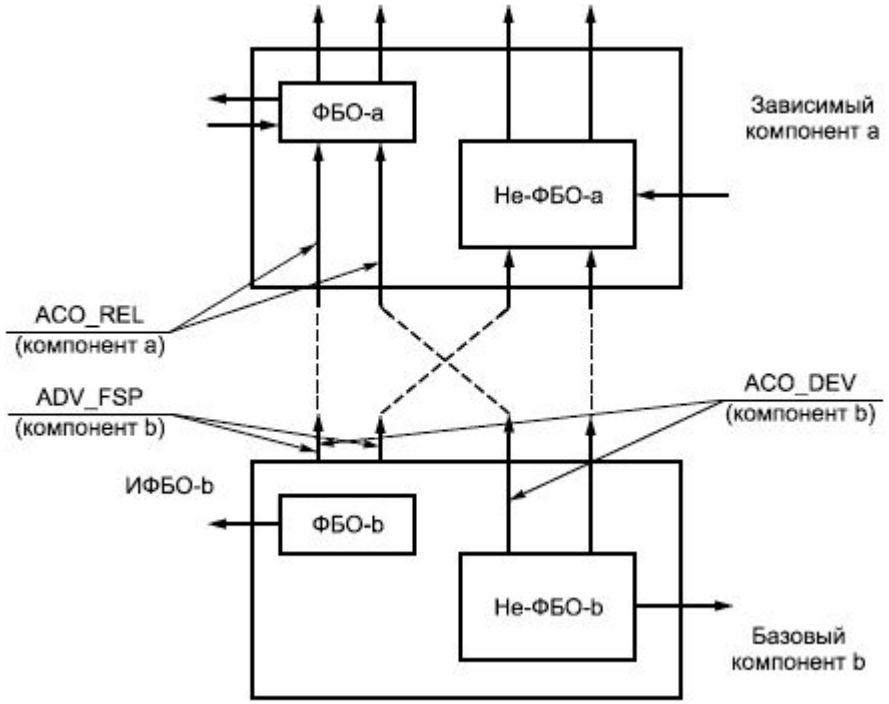
Семейства классов ATE, AVE и иерархия компонентов в семействах

Семейства класса ASO и иерархия компонентов в семействах, взаимодействие с другими классами





Семейства ASO



Компоненты ASO

Доклад окончен