4 класс (ОУДЗ+)

ADV_IMP.2 «Полное отображение представления реализации функциональных возможностей безопасности»
ADV_TDS.3 «Базовый модульный проект»
ADV_FSP.4 «Полная функциональная спецификация»
ALC_TAT.1 «Полностью определенные инструментальные средства разработки»
ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация»
ALC_FLR.1 «Базовое устранение недостатков»
AVA_VAN.5 «Усиленный методический анализ»
ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы»
AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы»
AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы»
AVA_CCA_EXT.1 «Анализ скрытых каналов»

ОУДЗ

ОУДЗ позволяет добросовестному разработчику достичь максимального доверия путем применения надлежащего проектирования безопасности на стадии разработки проекта без значительного изменения существующей практики качественной разработки.

ADV_ARC.1 Описание архитектуры безопасности
ADV_FSP.3 Функциональная спецификация с полной аннотацией
ADV_TDS.2 Архитектурный проект
AGD_OPE.1 Руководство пользователя по эксплуатации
AGD_PRE.1 Подготовительные процедуры
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_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_COV.2 Анализ покрытия
ATE_DPT.1 Тестирование: базовый проект
ATE_FUN.1 Функциональное тестирование
ATE_IND.2 Выборочное независимое тестирование
AVA_VAN.2 Анализ уязвимостей

3 класс (ОУД4+)

ADV_FSP.6 «Полная полуформальная функциональная спецификация с дополнительной формальной спецификацией»
ADV_IMP.2 «Полное отображение представления реализации функциональных возможностей безопасности»
ADV_SPM.1 «Формальная модель политики безопасности»
ALC_CMC.5 «Расширенная поддержка»
ALC_FLR.2 «Процедуры сообщений о недостатках»
AVA_VAN.5 «Усиленный методический анализ»
ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы»
AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы»
AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы»
AVA_CCA_EXT.1 «Анализ скрытых каналов»

ОУД4

ОУД4 позволяет разработчику достичь максимального доверия путем применения надлежащего проектирования безопасности, основанного на хороших коммерческих практиках разработки, которые, даже будучи строгими, не требуют глубоких профессиональных знаний, навыков и других ресурсов. ОУД4 — самый высокий уровень, на который, вероятно, экономически целесообразно ориентироваться при оценке уже существующих продуктов.

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_DPE.1 Руководство пользователя по эксплуатации
AGD_PRE.1 Подготовительные процедуры
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_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_COV.2 Анализ покрытия
ATE_DPT.2 Тестирование: модули обеспечения безопасности
ATE_FUN.1 Функциональное тестирование
ATE_IND.2 Выборочное независимое тестирование
AVA_VAN.3 Сосредоточенный анализ уязвимостей

2 класс (ОУД5+)

ADV_FSP.6 «Полная полуформальная функциональная спецификация с дополнительной формальной спецификацией»
ADV_IMP.2 «Полное отображение представления реализации функциональных возможностей безопасности»
ADV_SPM.1 «Формальная модель политики безопасности»
ALC_CMC.5 «Расширенная поддержка»
ALC_DVS.2 «Достаточность мер безопасности»
ALC_FLR.3 «Систематическое устранение недостатков»
AVA_VAN.5 «Усиленный методический анализ»
ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения операционной системы»
AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность операционной системы»
AMA_SIA_EXT.6 «Анализ влияния внешних модулей уровня ядра на безопасность операционной системы»
AVA_CCA_EXT.1 «Анализ скрытых каналов»

ОУД5

ОО будут, вероятно, проектироваться и разрабатываться с намерением достичь ОУД5.

ADV_ARC.1 Описание архитектуры безопасности
ADV_FSP5 Полная полуформальная спецификация с дополнительной информацией об ошибках
ADV_IMP1 Представление реализации ФБО
ADV_INT.2 Полностью определенная внутренняя структура
ADV_TDS.4 Полуформальный модульный проект
AGD_OPE.1 Руководство пользователя по эксплуатации
AGD_PRE.1 Подготовительные процедуры
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_TAT2 Соответствие стандартам реализации
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_COV.2 Анализ покрытия
ATE_DPT.3 Тестирование: модульный проект
ATE_FUN.1 Функциональное тестирование
ATE_IND.2 Выборочное независимое тестирование
AVA_VAN.4 Методический анализ уязвимостей

Класс AVA «Оценка уязвимостей». Анализ скрытых каналов (AVA_CCA_EXT)

Анализ скрытых каналов является частью анализа уязвимостей и проводится с целью сделать заключение о существовании и потенциальной пропускной способности каналов передачи сигналов (коммуникационных каналов), которые не предусмотрены для передачи защищаемой информации (данных пользователя и иной информации) или неразрешенных сигналов, но которые могут быть для этого использованы потенциальными нарушителями (в нарушение установленных политик управления информационными потоками, управления доступом или иных установленных ограничений).

В качестве скрытых каналов рассматриваются:

- каналы передачи, предназначенные для управления, но которые (в нарушение политики управления доступом или политики управления потоками) потенциально могут использоваться для передачи данных пользователя;
- каналы передачи, предназначенные для передачи данных пользователя, но которые потенциально могут использоваться для передачи сигналов нарушителя (в том числе с использованием модуляции передачи данных);
- каналы передачи, которые (в нарушение установленных ограничений) потенциально могут использоваться для наблюдения одним пользователем за действиями другого пользователя;
- иные типы скрытых каналов.
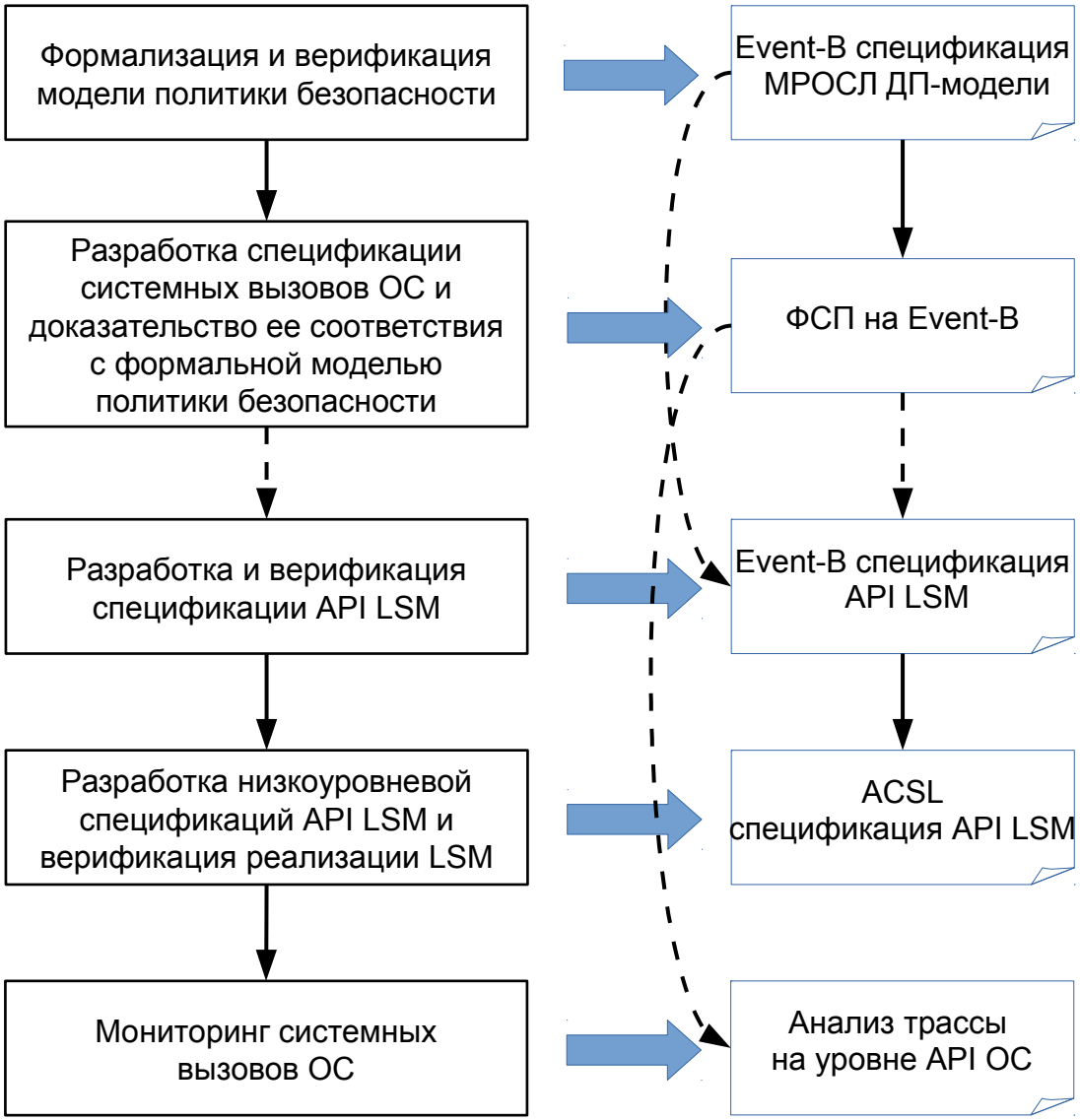
Схема процесса верификации механизма управления доступом ОС