РУСКРИПТО'2019

19 – 22 МАРТА, СОЛНЕЧНЫЙ PARK HOTEL & SPA

Сопоставление требований и практик применения ГОСТ Р ИСО/МЭК 15408 и КТ-178С

Хорошилов Алексей Владимирович
khoroshilov@ispras.ru

ИСП РАН

Институт системного программирования им. В.П. Иванникова
Российской академии наук

Ответственное ПО

- ПО, критичное с точки зрения **безопасности информации (security)**
- ПО, критичное с точки зрения **безопасности жизни (safety)**

Ответственное ПО

Ответственное ПО и сертификация

- ПО, критичное с точки зрения **безопасности информации (security)**
  - ГОСТ Р ИСО/МЭК 15408-2013. «Критерии оценки безопасности информационных технологий»
- ПО, критичное с точки зрения **безопасности жизни (safety)**
  - КТ-178С «Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техник»

ГОСТ Р 15408-3-2013 Критерии оценки безопасности ИТ

Задание по безопасности

- ASE_INT — Введение ЗБ
- ASE_CCL — Утверждение о соответствии
- ASE_SPD — Определение проблемы безопасности
- ASE_OBJ — Цели безопасности
- ASE_ECD — Определение расширенных компонентов
- ASE_REQ — Требования безопасности
- ASE_TSS — Краткая спецификация ОО

Разработка

- ADV_SPM — Моделирование политики безопасности
- ADV_FSP — Функциональная спецификация
- ADV_TDS — Проект ОО
- ADV_IMP — Представление реализации
- ADV_ARC — Архитектура безопасности
- ADV_INT — Внутренняя структура

Поддержка жизненного цикла

- ALC_CMC — Возможности УК
- ALC_CMS — Область УК
- ALC_DEL — Поставка
- ALC_DVS — Безопасность разработки
- ALC_FLR — Устранение недостатков
- ALC_LCD — Определение ЖЦ
- ALC_TAT — Инструменты и методы

Композиция

- ACO_COR — Обоснование композиции
- ACO_DEV — Свидетельство разработки
- ACO_REL — Зависимости компонентов
- ACO_CTT — Тестирование составного ОО
- ACO_VUL — Анализ уязвимостей композиции

Оценка уязвимостей

- AVA_VAN — Анализ уязвимостей

Тестирование

- ATE_COV — Покрытие
- ATE_FUN — Функциональное тестирование
- ATE_DPT — Глубина
- ATE_IND — Независимое тестирование

Руководства

- AGD_OPE — Руководство по эксплуатации
- AGD_PRE — Подготовительные процедуры

КТ-178С Требования к ПО бортовой аппаратуры и систем

Анализ безопасности

- P-4754A Оценка безопасности системы

Процесс планирования

- План сертификации
- План разработки
- План управления конфигурацией
- План гарантии качества
- Планирование среды ЖЦ
- Стандарт на разработку требований
- Стандарт на проектирование
- Стандарт на кодирование

Разработка

- Процесс разработки требований
- Процесс проектирования
- Процесс кодирования
- Процесс интеграции

Верификация

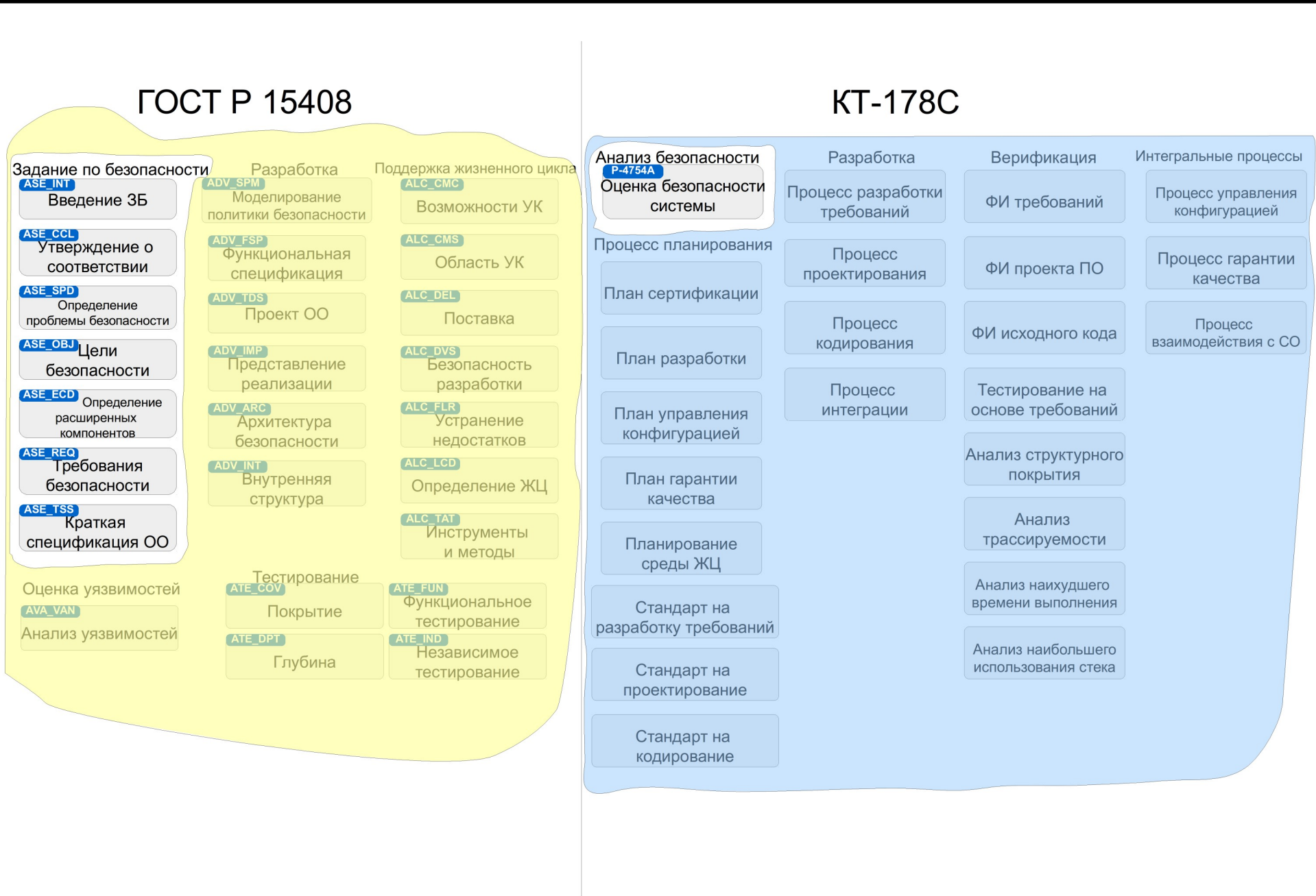
- ФИ требований
- ФИ проекта ПО
- ФИ исходного кода
- Тестирование на основе требований
- Анализ структурного покрытия
- Анализ трассируемости
- Анализ наихудшего времени выполнения
- Анализ наибольшего использования стека

Интегральные процессы

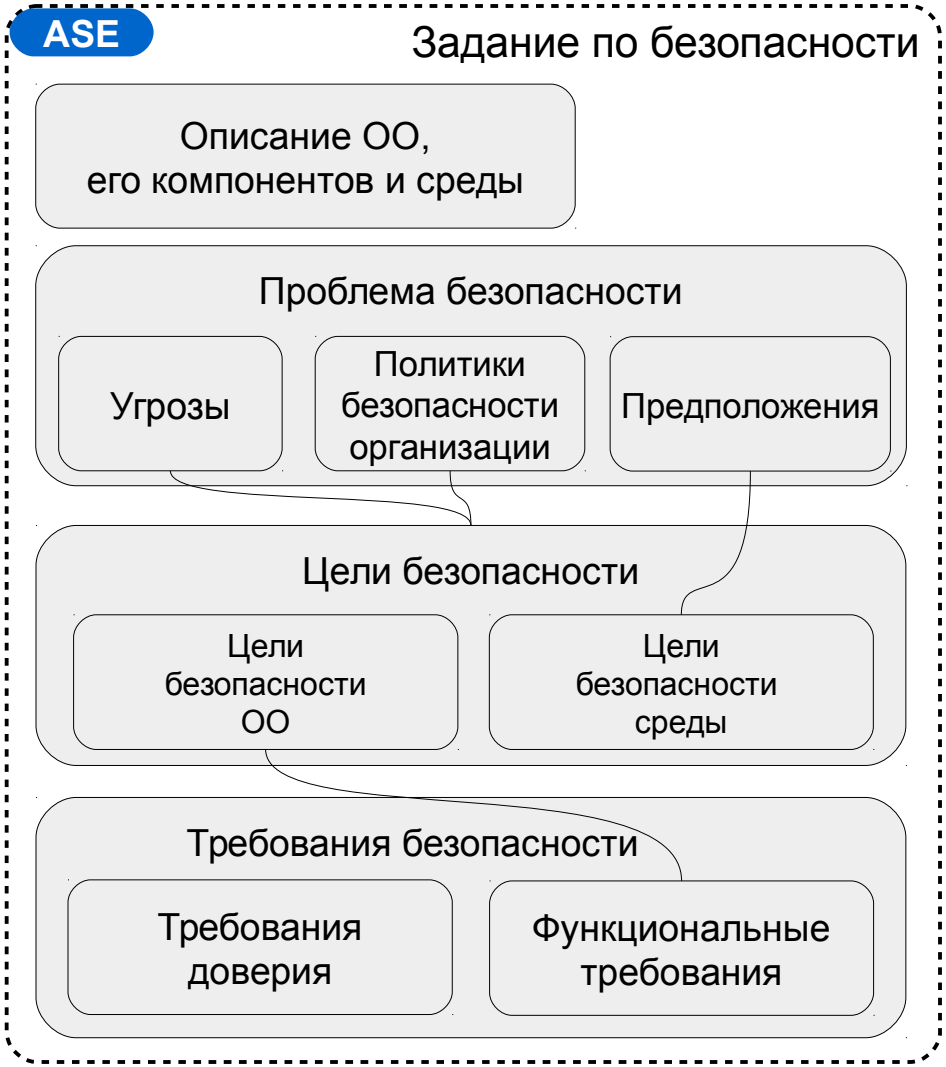
- Процесс управления конфигурацией
- Процесс гарантии качества
- Процесс взаимодействия с СО

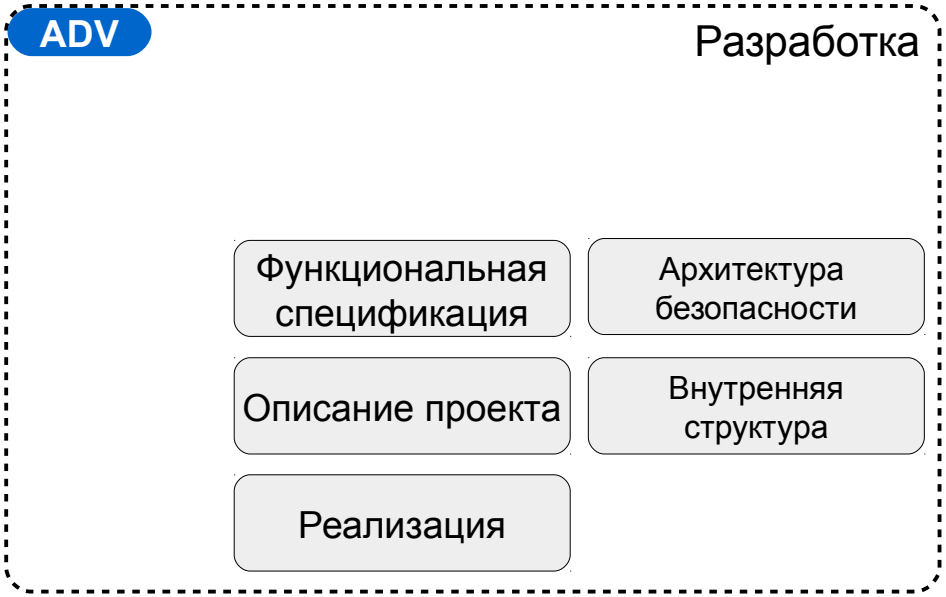
Security vs Safety

- Общая цель:
  - обеспечение безопасности, т. е. корректной реализации функций безопасности
- Отличие:
  - распределение вероятностей негативных событий


ГОСТ Р 15408
Задание по безопасности
ASE_INT
Введение ЗБ
ASE_CCL
Утверждение о соответствии
ASE_SPD
Определение проблемы безопасности
ASE_OBJ
Цели безопасности
ASE_ECD
Определение расширенных компонентов
ASE_REQ
Требования безопасности
ASE_TSS
Краткая спецификация ОО
Разработка
ADV_SPM
Моделирование политики безопасности
ADV_FSP
Функциональная спецификация
ADV_TDS
Проект ОО
ADV_IMP
Представление реализации
ADV_ARC
Архитектура безопасности
ADV_INT
Внутренняя структура
Поддержка жизненного цикла
ALC_CMC
Возможности УК
ALC_CMS
Область УК
ALC_DEL
Поставка
ALC_DVS
Безопасность разработки
ALC_FLR
Устранение недостатков
ALC_LCD
Определение ЖЦ
ALC_TAT
Инструменты и методы
Оценка уязвимостей
AVA_VAN
Анализ уязвимостей
Тестирование
ATE_COV
Покрытие
ATE_DPT
Глубина
ATE_FUN
Функциональное тестирование
ATE_IND
Независимое тестирование
КТ-178С
Анализ безопасности
P-4754A
Оценка безопасности системы
Процесс планирования
План сертификации
План разработки
План управления конфигурацией
План гарантии качества
Планирование среды ЖЦ
Стандарт на разработку требований
Стандарт на проектирование
Стандарт на кодирование
Разработка
Процесс разработки требований
Процесс проектирования
Процесс кодирования
Процесс интеграции
Верификация
ФИ требований
ФИ проекта ПО
ФИ исходного кода
Тестирование на основе требований
Анализ структурного покрытия
Анализ трассируемости
Анализ наихудшего времени выполнения
Анализ наибольшего использования стека
Интегральные процессы
Процесс управления конфигурацией
Процесс гарантии качества
Процесс взаимодействия с СО

ГОСТ Р 15408-3-2013 Задание по безопасности





КТ-178С: Ошибки в ПО и отказные состояния уровня ВС

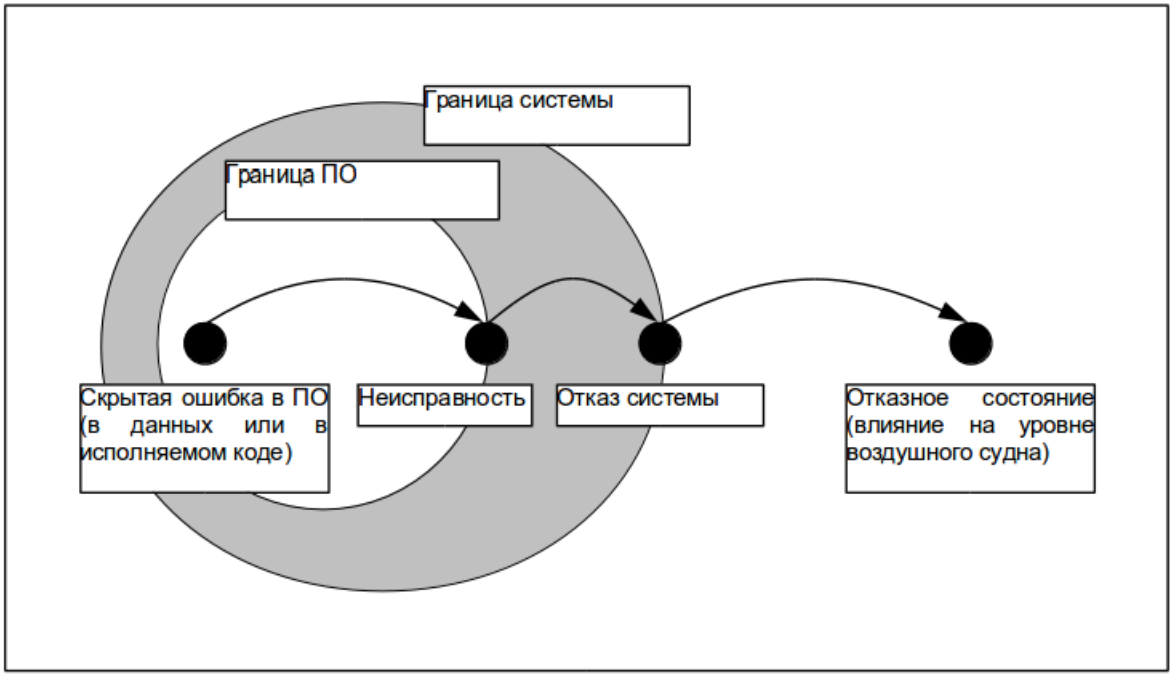
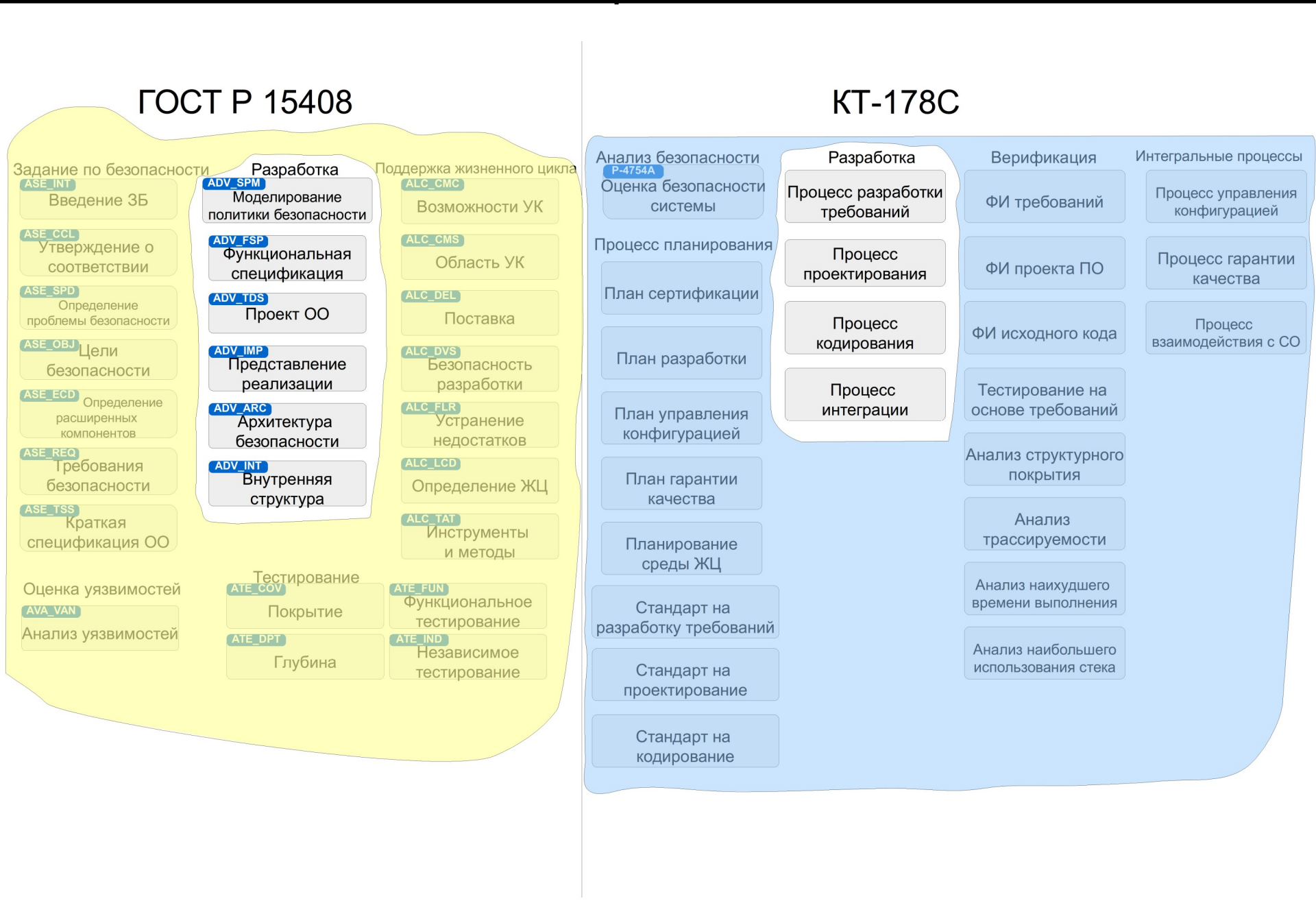


Рисунок 2-2. Последовательность событий для ошибки в ПО, ведущей к отказному состоянию

КТ-178С: категории отказных состояний

- **Катастрофические**
  - Многочисленные жертвы, обычно с потерей ВС
- **Аварийные**
  - значительное снижение запасов по безопасности или функциональных возможностей
  - серьезные или смертельные ранения относительно небольшого числа находящихся на борту людей, не входящих в летный экипаж
- **Сложные (значительные)**
  - заметное снижение запасов по безопасности или функциональных возможностей
  - заметное увеличение рабочей нагрузки на экипаж или появление условий, понижающих эффективность работы экипажа
  - дискомфорт для летного экипажа или ухудшение условий для пассажиров или бортпроводников, возможно, с причинением травм
- **Усложнение условий полета (незначительные)**
  - незначительным снижением запасов по безопасности или функциональных возможностей
  - незначительным увеличением рабочей нагрузки на экипаж
  - некоторым физическим дискомфортом для пассажиров или бортпроводников


ГОСТ Р 15408
Задание по безопасности
ASE_INT
Введение ЗБ
ASE_CCL
Утверждение о соответствии
ASE_SPD
Определение проблемы безопасности
ASE_OBJ
Цели безопасности
ASE_ECD
Определение расширенных компонентов
ASE_REQ
Требования безопасности
ASE_TSS
Краткая спецификация ОО
Разработка
ADV_SPM
Моделирование политики безопасности
ADV_FSP
Функциональная спецификация
ADV_TDS
Проект ОО
ADV_IMP
Представление реализации
ADV_ARC
Архитектура безопасности
ADV_INT
Внутренняя структура
Поддержка жизненного цикла
ALC_CMC
Возможности УК
ALC_CMS
Область УК
ALC_DEL
Поставка
ALC_DVS
Безопасность разработки
ALC_FLR
Устранение недостатков
ALC_LCD
Определение ЖЦ
ALC_TAT
Инструменты и методы
Оценка уязвимостей
AVA_VAN
Анализ уязвимостей
Тестирование
ATE_COV
Покрытие
ATE_DPT
Глубина
ATE_FUN
Функциональное тестирование
ATE_IND
Независимое тестирование
КТ-178С
Анализ безопасности
P-4754A
Оценка безопасности системы
Процесс планирования
План сертификации
План разработки
План управления конфигурацией
План гарантии качества
Планирование среды ЖЦ
Стандарт на разработку требований
Стандарт на проектирование
Стандарт на кодирование
Разработка
Процесс разработки требований
Процесс проектирования
Процесс кодирования
Процесс интеграции
Верификация
ФИ требований
ФИ проекта ПО
ФИ исходного кода
Тестирование на основе требований
Анализ структурного покрытия
Анализ трассируемости
Анализ наихудшего времени выполнения
Анализ наибольшего использования стека
Интегральные процессы
Процесс управления конфигурацией
Процесс гарантии качества
Процесс взаимодействия с СО

ГОСТ Р 15408-3-2013 Вопросы разработки

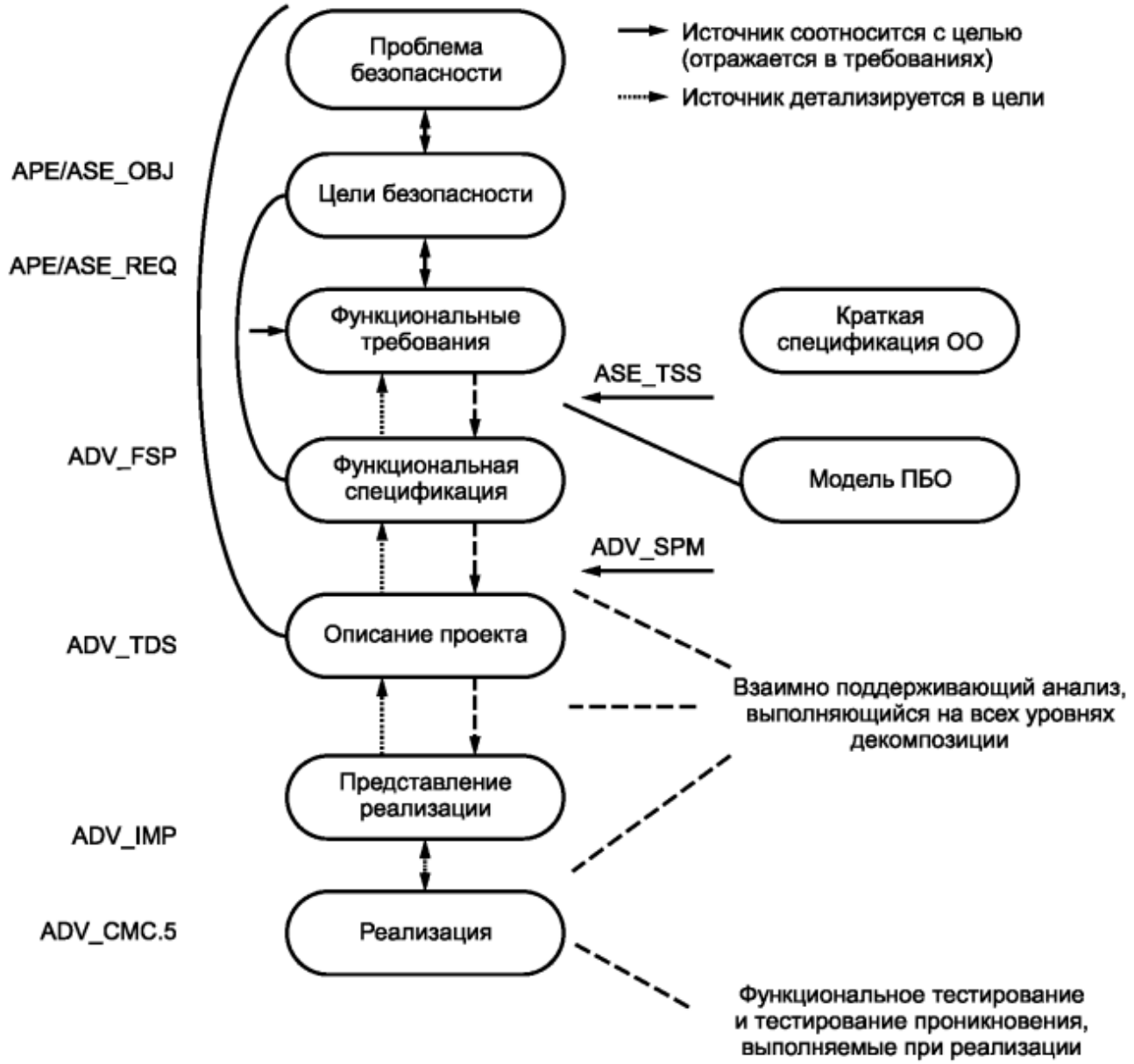
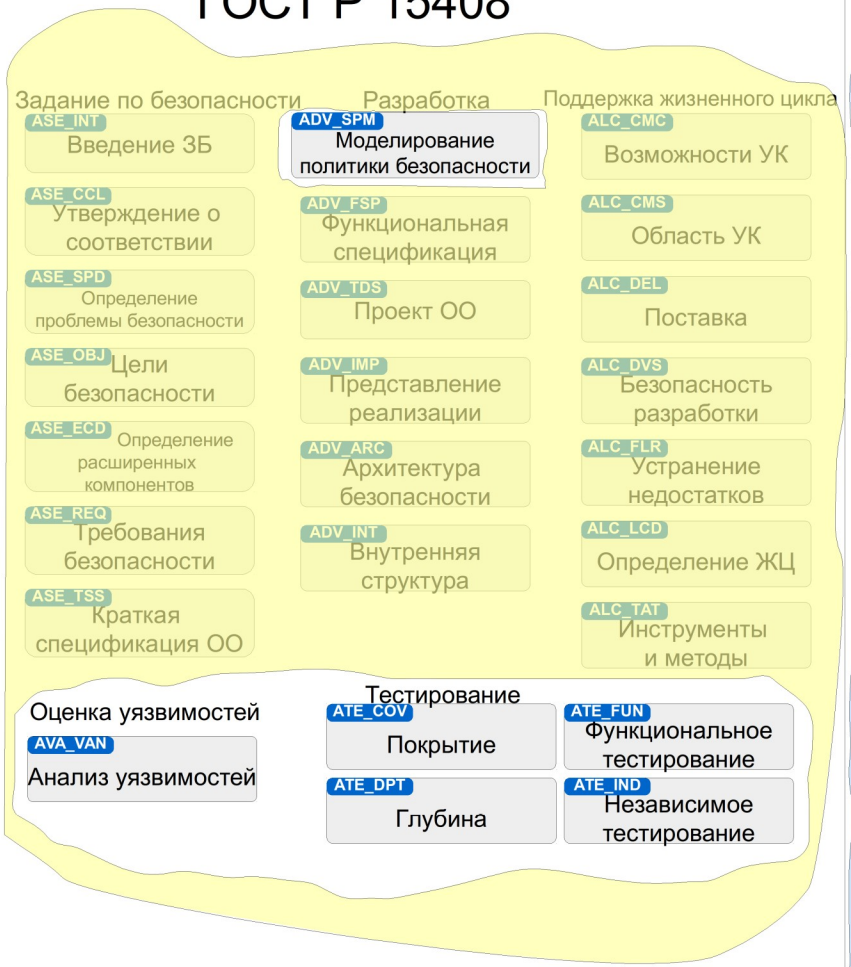


Рисунок 10 — Взаимосвязи между компонентами класса ADV и с другими семействами

ГОСТ Р 15408



КТ-178С

Руководство Р-333
«Дополнение по формальным методам
к документам КТ-178С и КТ-278А»

КТ-178С: Тестирование

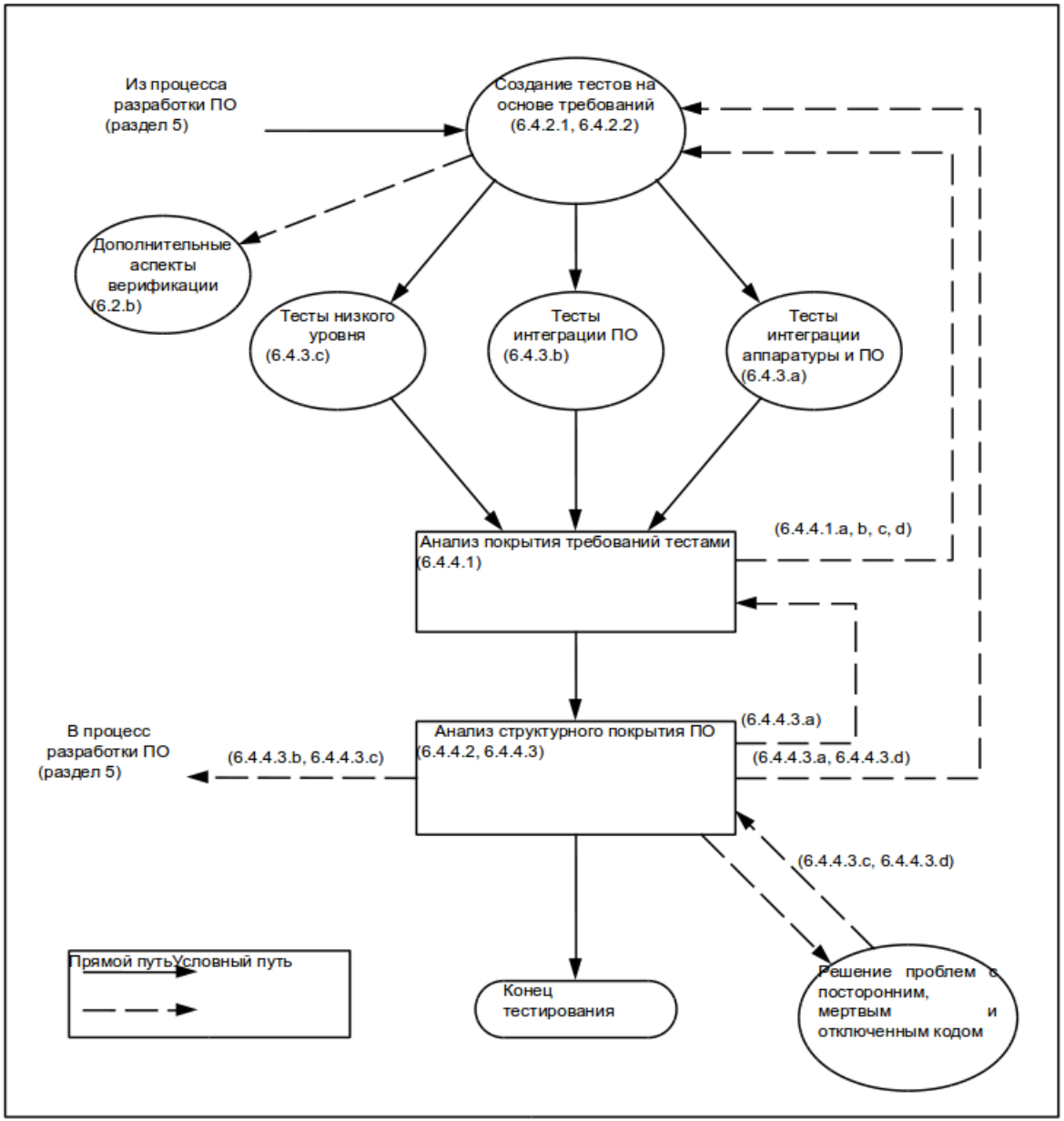
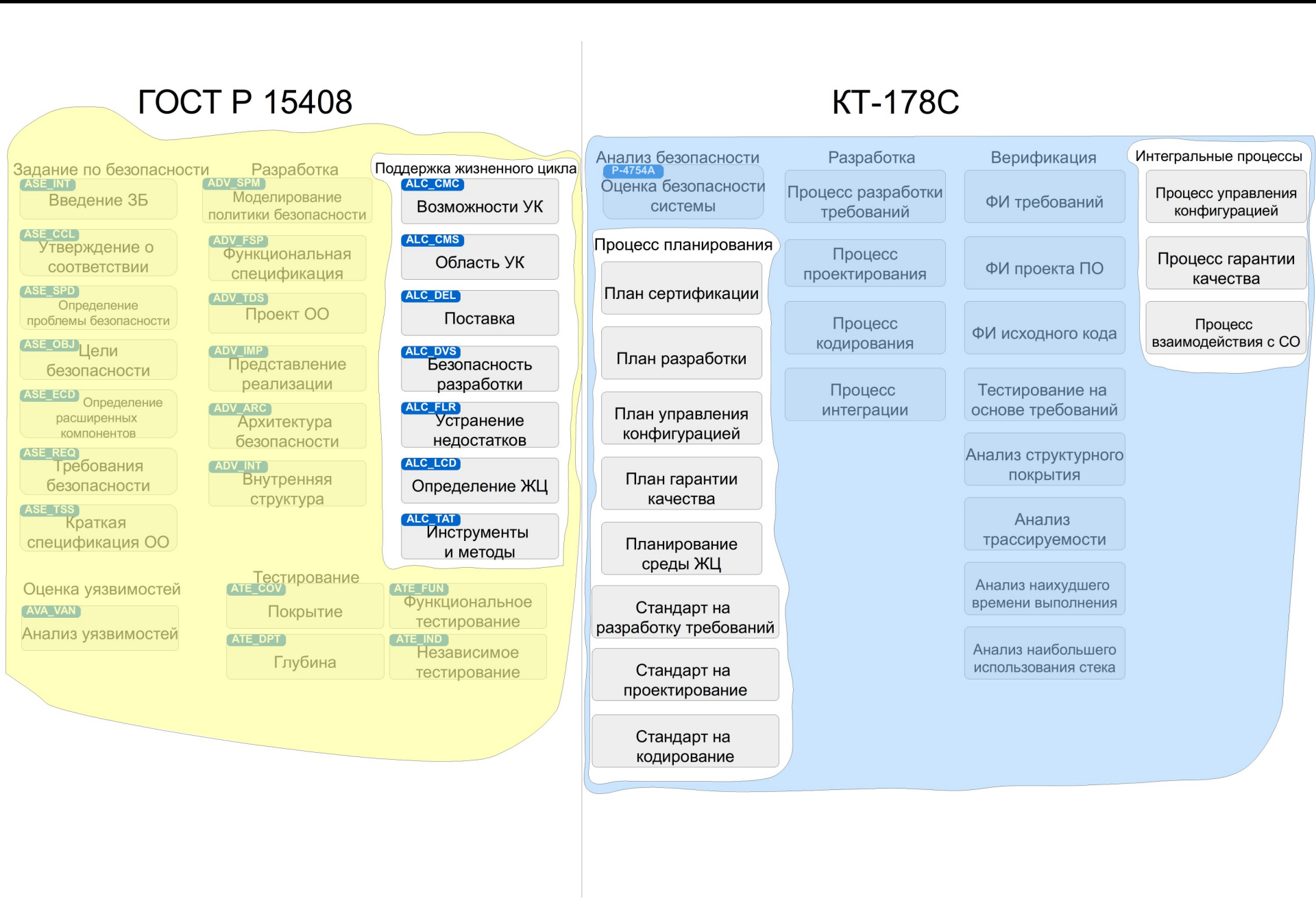


Рисунок 6-1. Мероприятия тестирования ПО


ГОСТ Р 15408
Задание по безопасности
ASE_INT
Введение ЗБ
ASE_CCL
Утверждение о соответствии
ASE_SPD
Определение проблемы безопасности
ASE_OBJ
Цели безопасности
ASE_ECD
Определение расширенных компонентов
ASE_REQ
Требования безопасности
ASE_TSS
Краткая спецификация ОО
Разработка
ADV_SPM
Моделирование политики безопасности
ADV_FSP
Функциональная спецификация
ADV_TDS
Проект ОО
ADV_IMP
Представление реализации
ADV_ARC
Архитектура безопасности
ADV_INT
Внутренняя структура
Поддержка жизненного цикла
ALC_CMC
Возможности УК
ALC_CMS
Область УК
ALC_DEL
Поставка
ALC_DVS
Безопасность разработки
ALC_FLR
Устранение недостатков
ALC_LCD
Определение ЖЦ
ALC_TAT
Инструменты и методы
Оценка уязвимостей
AVA_VAN
Анализ уязвимостей
Тестирование
ATE_COV
Покрытие
ATE_DPT
Глубина
ATE_FUN
Функциональное тестирование
ATE_IND
Независимое тестирование
КТ-178С
Анализ безопасности
P-4754A
Оценка безопасности системы
Процесс планирования
План сертификации
План разработки
План управления конфигурацией
План гарантии качества
Планирование среды ЖЦ
Стандарт на разработку требований
Стандарт на проектирование
Стандарт на кодирование
Разработка
Процесс разработки требований
Процесс проектирования
Процесс кодирования
Процесс интеграции
Верификация
ФИ требований
ФИ проекта ПО
ФИ исходного кода
Тестирование на основе требований
Анализ структурного покрытия
Анализ трассируемости
Анализ наихудшего времени выполнения
Анализ наибольшего использования стека
Интегральные процессы
Процесс управления конфигурацией
Процесс гарантии качества
Процесс взаимодействия с СО

ГОСТ Р 56939-2016 «Разработка безопасного ПО»

- Анализ требований
  - каталог требований по безопасности
- Проектирование архитектуры
  - моделирование угроз безопасности
- Конструирование и комплексирование
  - идентифицированы инструментальные средства
  - требования к кодированию
  - экспертиза (для важных подкомпонентов)
  - статический анализатор
- Квалификационное тестирование
  - функциональное тестирование
  - тестирование на проникновение
  - динамический анализ кода программы
  - фаззинг
- Инсталяция и приемка
- Эксплуатация
- Менеджмент документация и конфигурация
- Менеджмент инфраструктурной среды
- Менеджмент людскими ресурсами

Заключение

- ГОСТ Р 15408
  - в т.ч. сертификация переиспользуемых компонентов
  - в т.ч. большие системы
- КТ-178С
  - сертификация только воздушного судна
  - полностью контролируемая разработка

Заключение

- КТ-178С → ГОСТ Р 15408
  - тестирование/структурное покрытия
  - требования
  - трассируемость
- ГОСТ Р 56939 → КТ-178С
  - статический анализ
  - фаззинг
  - санитайзеры

LinuxTesting.org

Спасибо!

Хорошилов Алексей Владимирович
khoroshilov@ispras.ru

ИСП РАН
Институт системного программирования им. В.П. Иванникова
Российской академии наук