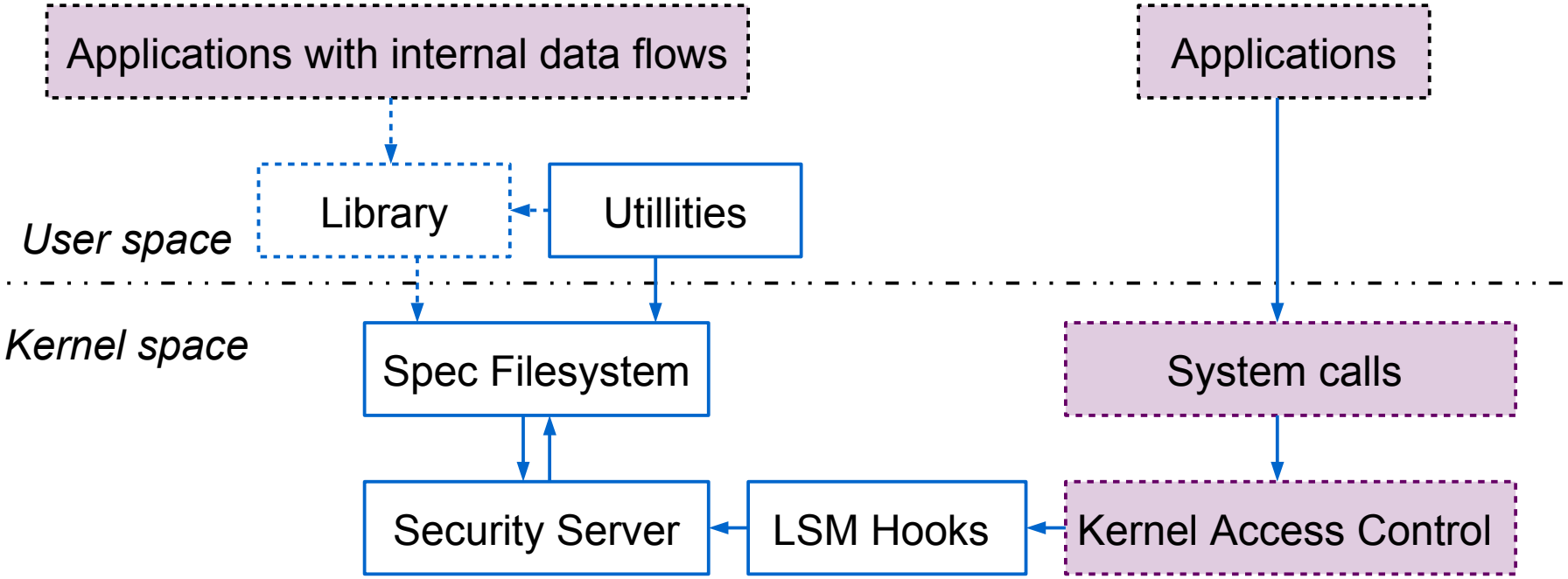
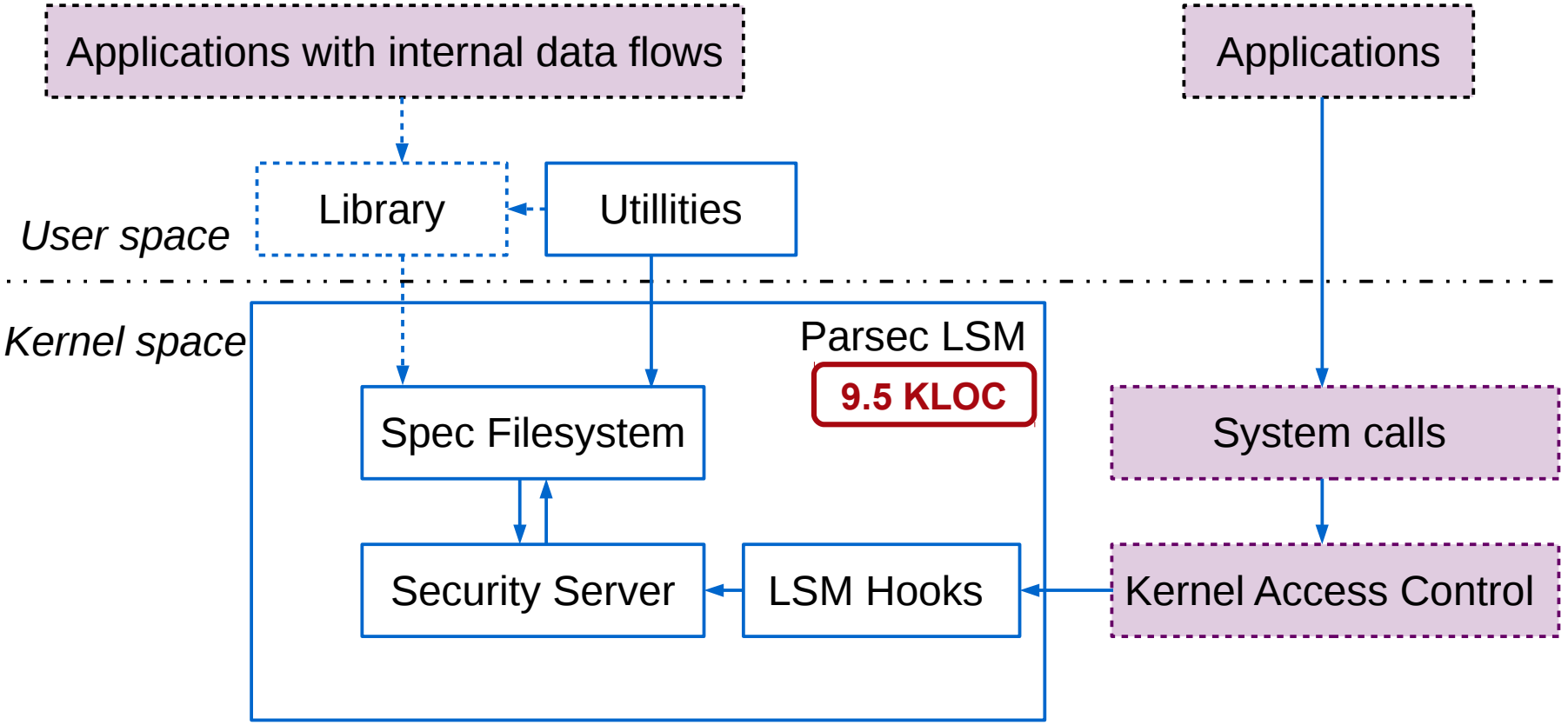
Анализ сложности верификации средств защиты информации в различных архитектурах защищённых ОС Linux

А. Хорошилов (ИСП РАН)

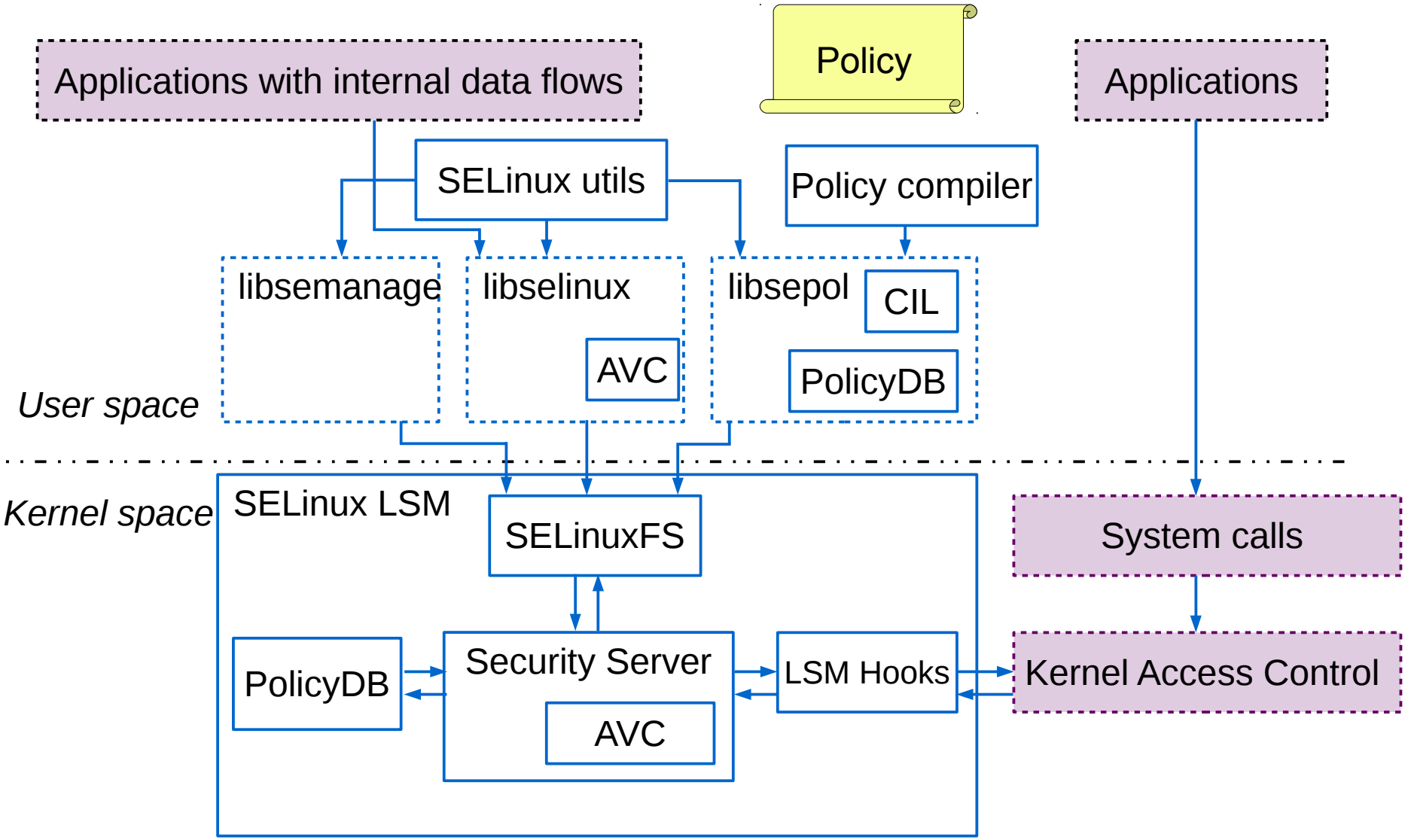
Общая архитектура



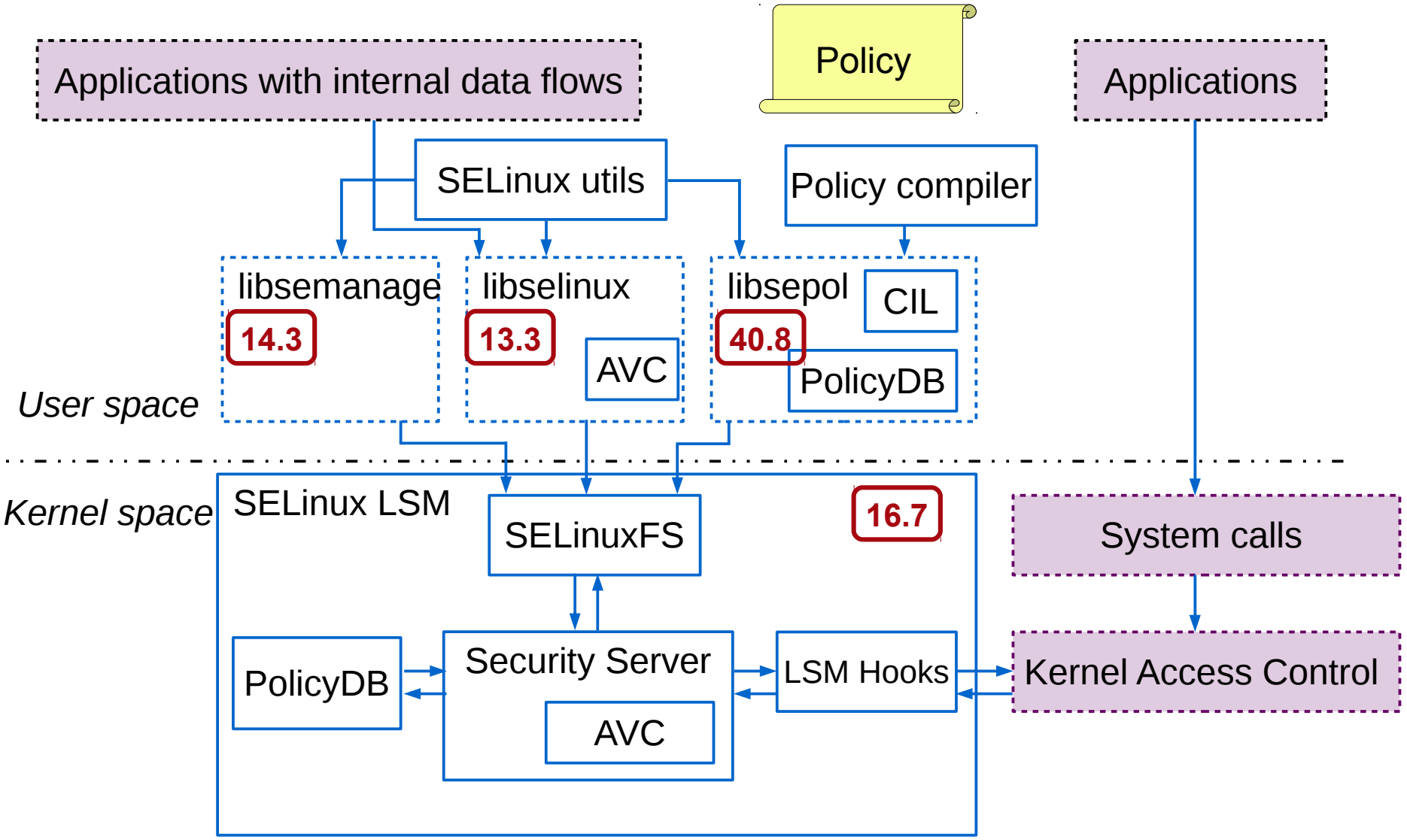
Компоненты parsec



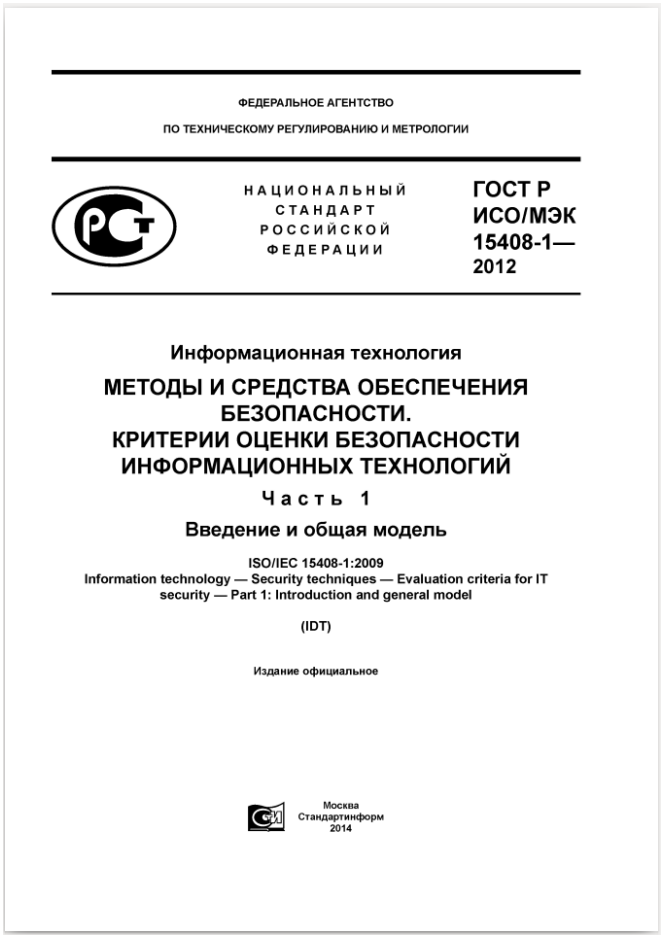
Компоненты SELinux



Компоненты SELinux



ГОСТ Р 15408-2013 Критерии оценки безопасности ИТ



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-1— 2012

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 1

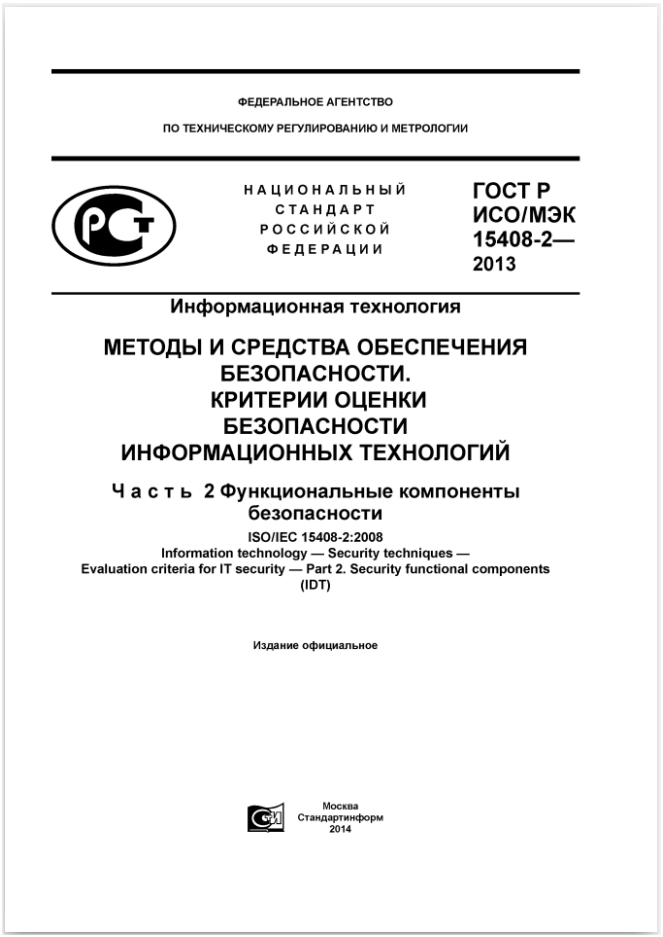
Введение и общая модель

ISO/IEC 15408-1:2009
Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

(IDT)

Издание официальное

Москва
Стандартинформ
2014



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-2— 2013

Информационная технология

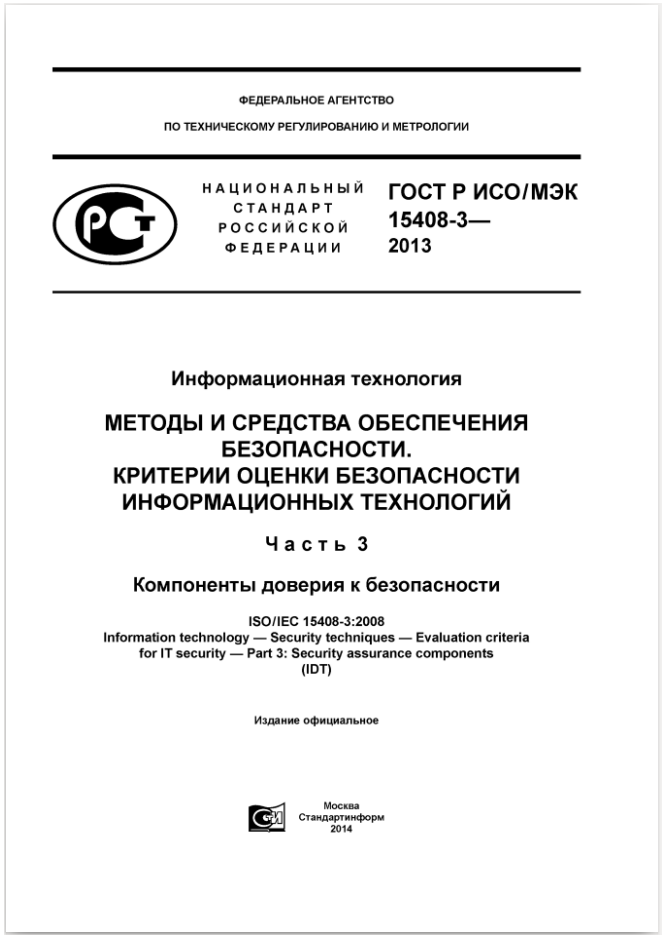
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 2 Функциональные компоненты безопасности

ISO/IEC 15408-2:2008
Information technology — Security techniques — Evaluation criteria for IT security — Part 2. Security functional components
(IDT)

Издание официальное

Москва
Стандартинформ
2014



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-3— 2013

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 3

Компоненты доверия к безопасности

ISO/IEC 15408-3:2008
Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
(IDT)

Издание официальное

Москва
Стандартинформ
2014

Компоненты доверия к безопасности (ГОСТ Р 15408-3-2013)

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

Тестирование

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

Оценка уязвимостей

- **AVA_VAN** Анализ уязвимостей

Руководства

- **AGD_OPE** Руководство по эксплуатации
- **AGD_PRE** Подготовительные процедуры

Процесс моделирования и верификации ПБ

- ADV_SPM.1 «Формальная модель политики безопасности»
- ADV_FSP.6 «Полная полуформальная функциональная спецификация с дополнительной формальной спецификацией»
- AVA_CCA_EXT.1 «Анализ скрытых каналов»

«Профиль защиты операционных систем типа «А» второго класса защиты ИТ.ОС.А2.ПЗ» (ФСТЭК России, 2016)

Компоненты доверия к безопасности (ГОСТ Р 15408-3-2013)

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

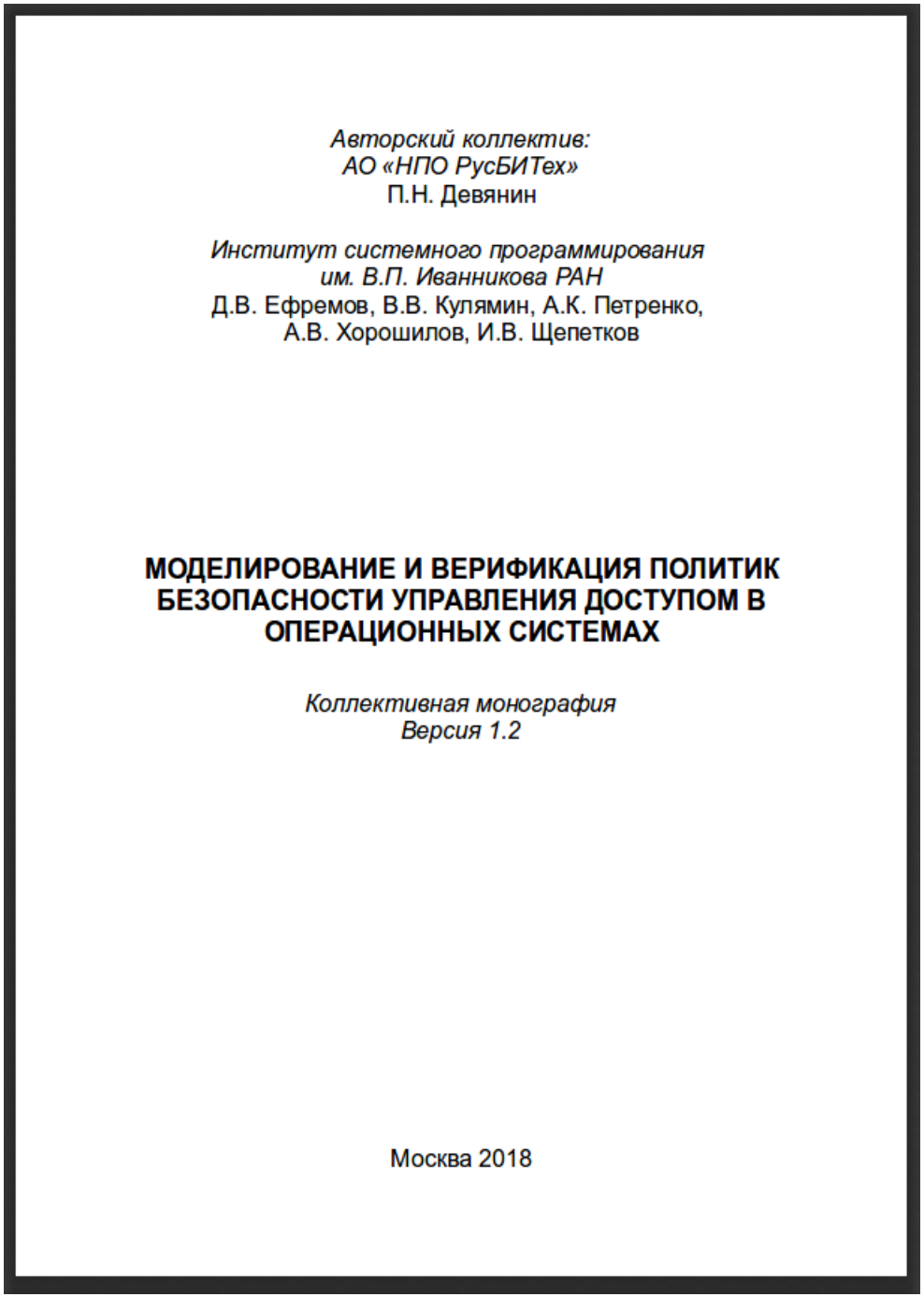
- **AVA_VAN** Анализ уязвимостей

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

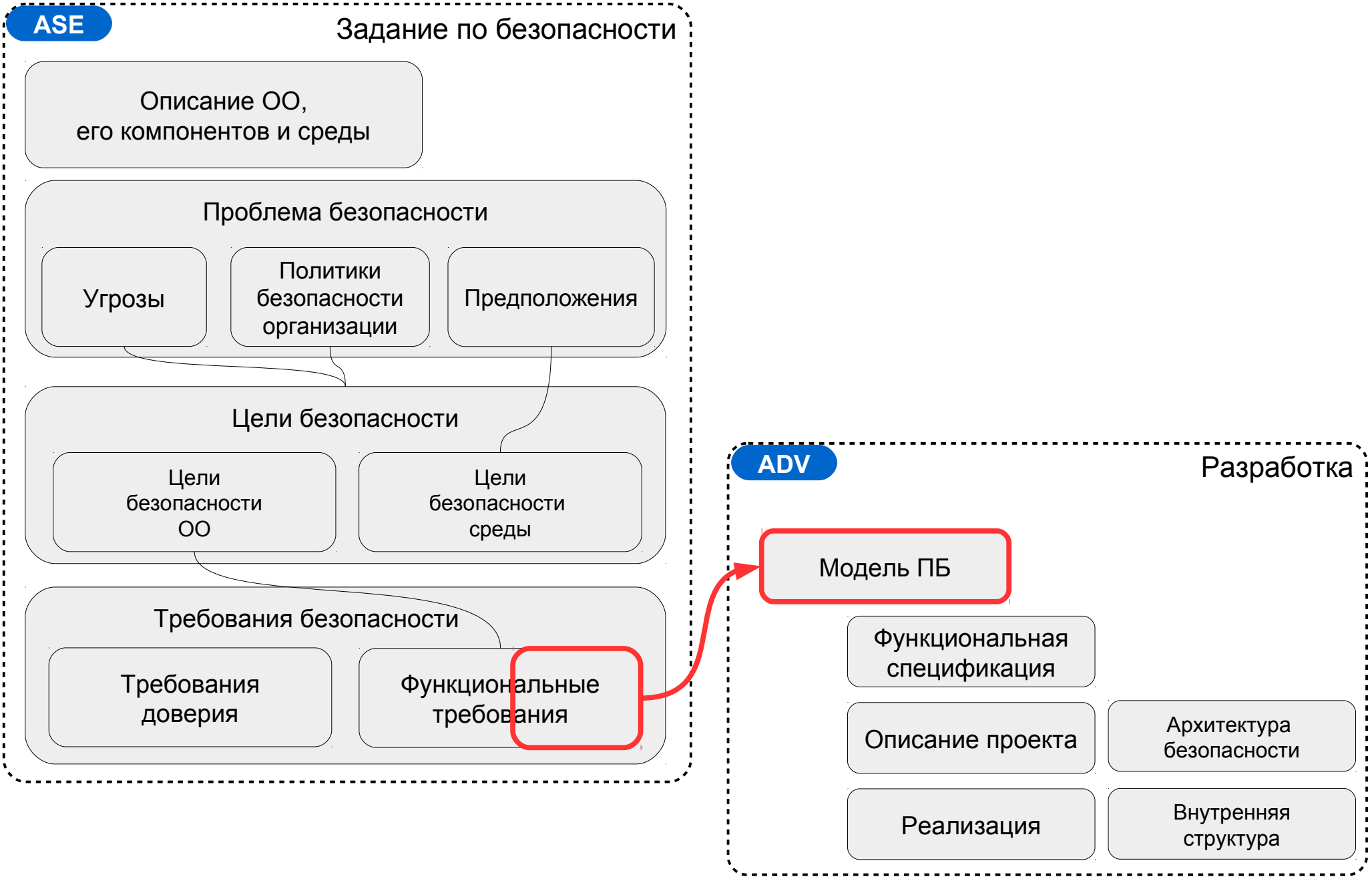


П.Н. Девянин, Д.В. Ефремов, В.В. Кулямин, А.К. Петренко, А.В. Хорошилов, И.В. Щепетков
Моделирование и верификация политик безопасности управления доступом в операционных системах
http://www.ispras.ru/publications/2018/security_policy_modeling_and_verification/

Процесс моделирования и верификации ПБ

- 1. Моделирование ПБ
  - 1.1 Разработка модели ПБ в математической нотации
  - 1.2 Описание модели ПБ в нотации Event-B
  - 1.3 Верификация модели ПБ в нотации Event-B
- 2. Функциональная спецификация
  - 2.1 Формализация функциональной спецификации
  - 2.2 Верификация функциональной спецификации
- 3. Верификация реализации
  - 3.1 Дедуктивная верификация ключевых компонентов
    - 3.1.1 Выделение ключевых компонентов
    - 3.1.2 Спецификация требований к компоненту и его окружению
    - 3.1.3 Дедуктивная верификация компонентов
  - 3.2 Тестирование реализации
    - 3.2.1 Мониторинг соответствия модели ФСП

ADV_SPM - Моделирование политики безопасности



Цели моделирования ПБ

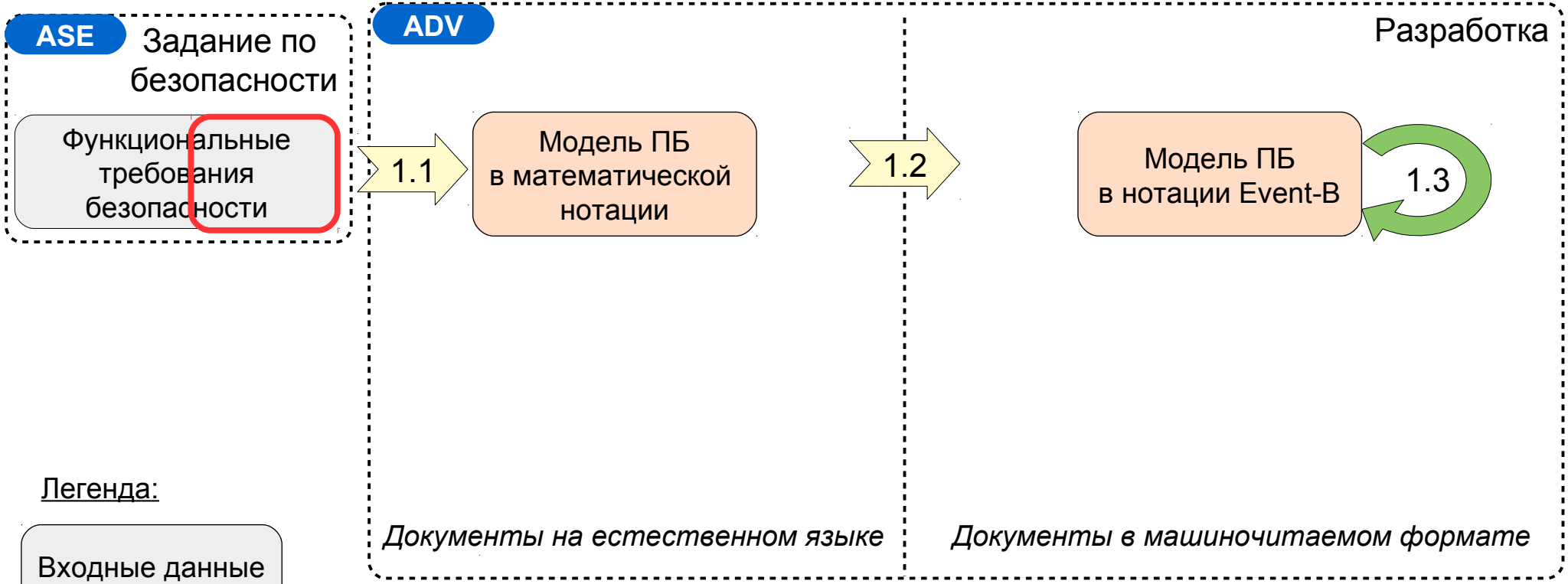
повышение доверия за счёт

- наличия формальной модели политики безопасности, снижающей риски
  - неправильного понимания требований
  - неверной реализации требований
- установления соответствия между функциональной спецификацией и этой моделью

Формальная верификация

- доказательство отсутствия внутренних противоречий в модели ПБ
- доказательство недостижимости "небезопасных" состояний
- доказательство соответствия между формальной функциональной спецификацией и моделью ПБ

Процесс моделирования и верификации ПБ



Легенда:

Входные данные процесса

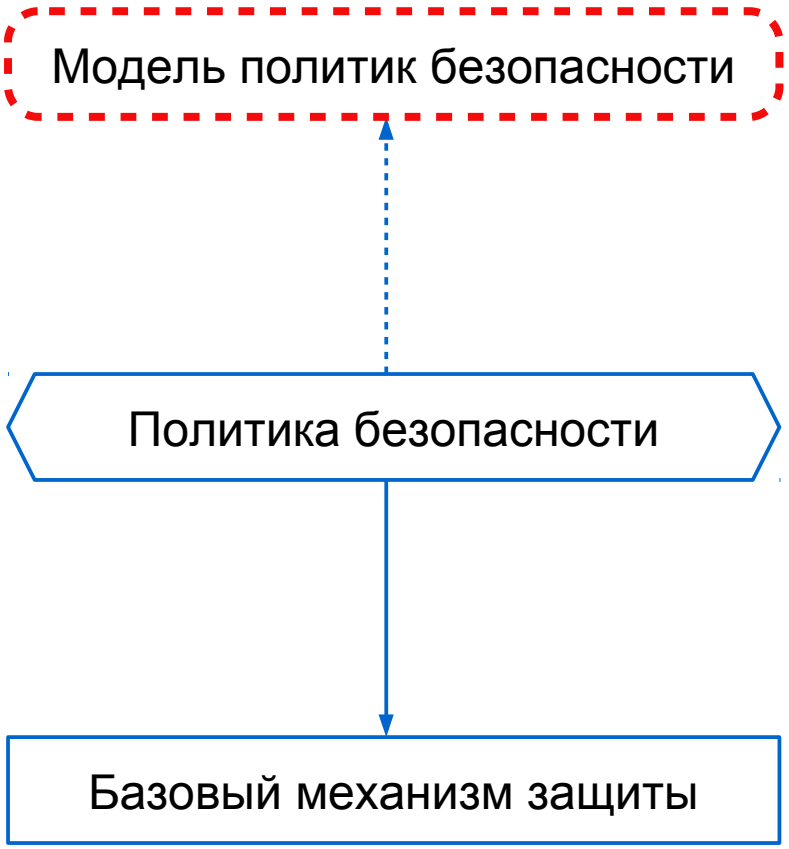
Результат процесса

Ручная разработка

Автоматизированная верификация

- 1. Моделирование ПБ
  - 1.1 Разработка модели ПБ в математической нотации
  - 1.2 Описание модели ПБ в нотации Event-B
  - 1.3 Верификация модели ПБ в нотации Event-B
    - доказательство отсутствия внутренних противоречий в модели ПБ
    - доказательство недостижимости "небезопасных" состояний

Модель политики безопасности



Свойства безопасности, основные функциональные возможности, общая структура меток, абстрактные операции

Набор значений меток (пользователей, ролей, уровней и пр.), разметка объектов, правила разметки процессов и новых объектов, конкретные правила контроля доступа

Конкретная структура меток, конкретные операции, общие правила контроля доступа

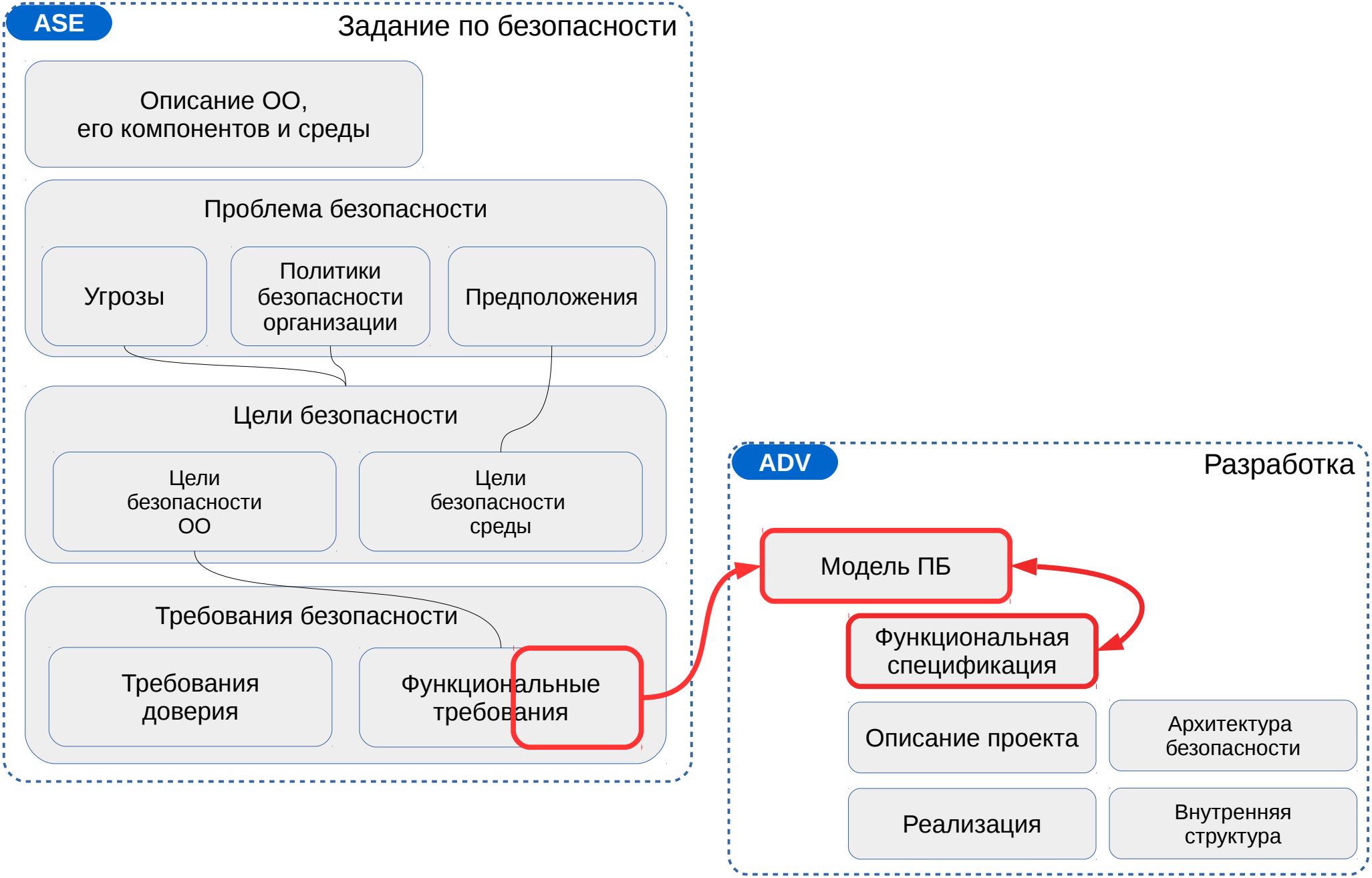
Процесс моделирования и верификации ПБ

- 1. Моделирование ПБ
  - 1.1 Разработка модели ПБ в математической нотации
  - 1.2 Описание модели ПБ в нотации Event-B
  - 1.3 Верификация модели ПБ в нотации Event-B
- 2. Функциональная спецификация
  - 2.1 Формализация функциональной спецификации
  - 2.2 Верификация функциональной спецификации
- 3. Верификация реализации
  - 3.1 Дедуктивная верификация ключевых компонентов
    - 3.1.1 Выделение ключевых компонентов
    - 3.1.2 Спецификация требований к компоненту и его окружению
    - 3.1.3 Дедуктивная верификация компонентов
  - 3.2 Тестирование реализации
    - 3.2.1 Мониторинг соответствия модели ФСП

Процесс моделирования и верификации ПБ

- 1. Моделирование ПБ
  - 1.1 Разработка модели ПБ в математической нотации
  - 1.2 Описание модели ПБ в нотации Event-B
  - 1.3 Верификация модели ПБ в нотации Event-B
- 2. Функциональная спецификация
  - 2.1 Формализация функциональной спецификации
  - 2.2 Верификация функциональной спецификации
- 3. Верификация реализации
  - 3.1 Дедуктивная верификация ключевых компонентов
    - 3.1.1 Выделение ключевых компонентов
    - 3.1.2 Спецификация требований к компоненту и его окружению
    - 3.1.3 Дедуктивная верификация компонентов
  - 3.2 Тестирование реализации
    - 3.2.1 Мониторинг соответствия модели ФСП

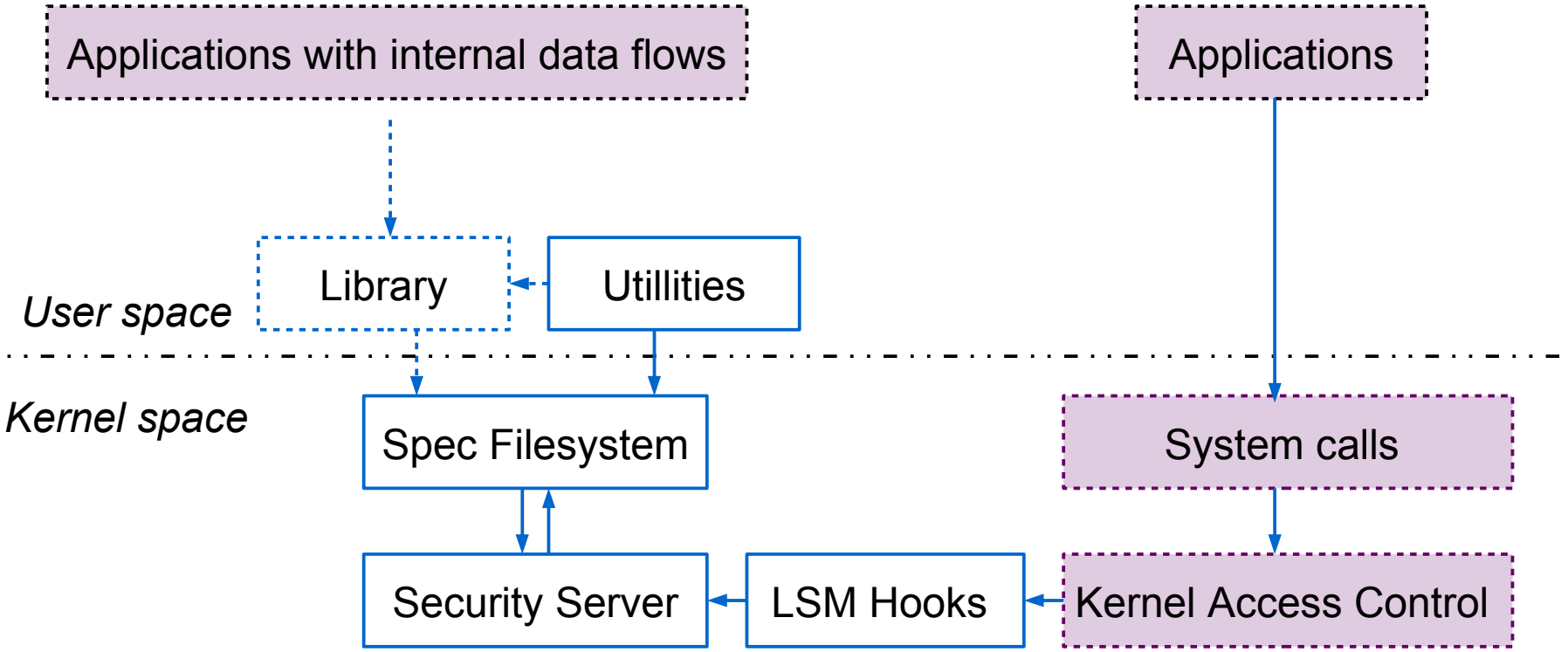
ГОСТ Р 15408-3-2013 Критерии оценки безопасности ИТ



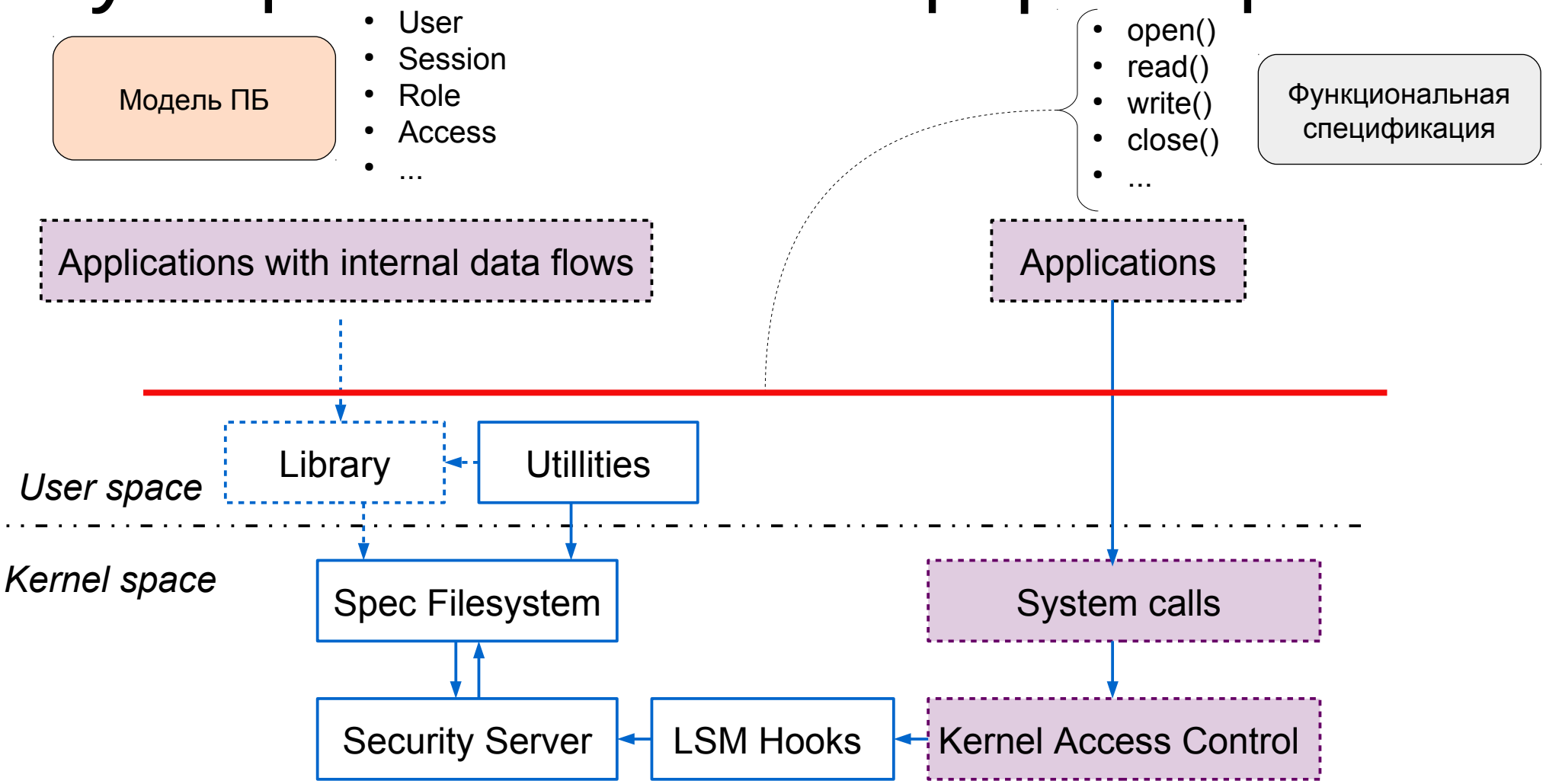
Функциональная спецификация ОС

Модель ПБ

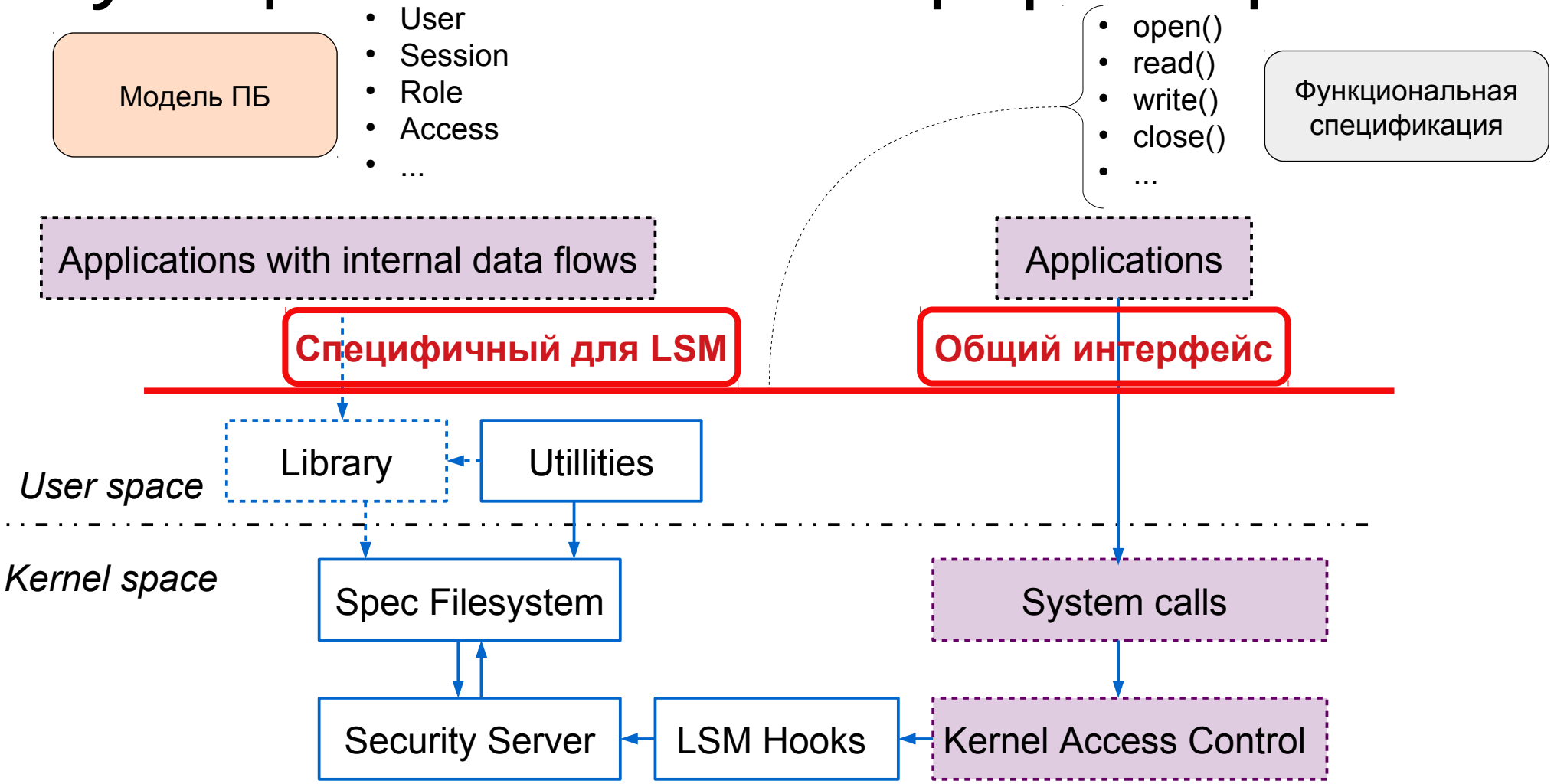
- User
- Session
- Role
- Access
- ...



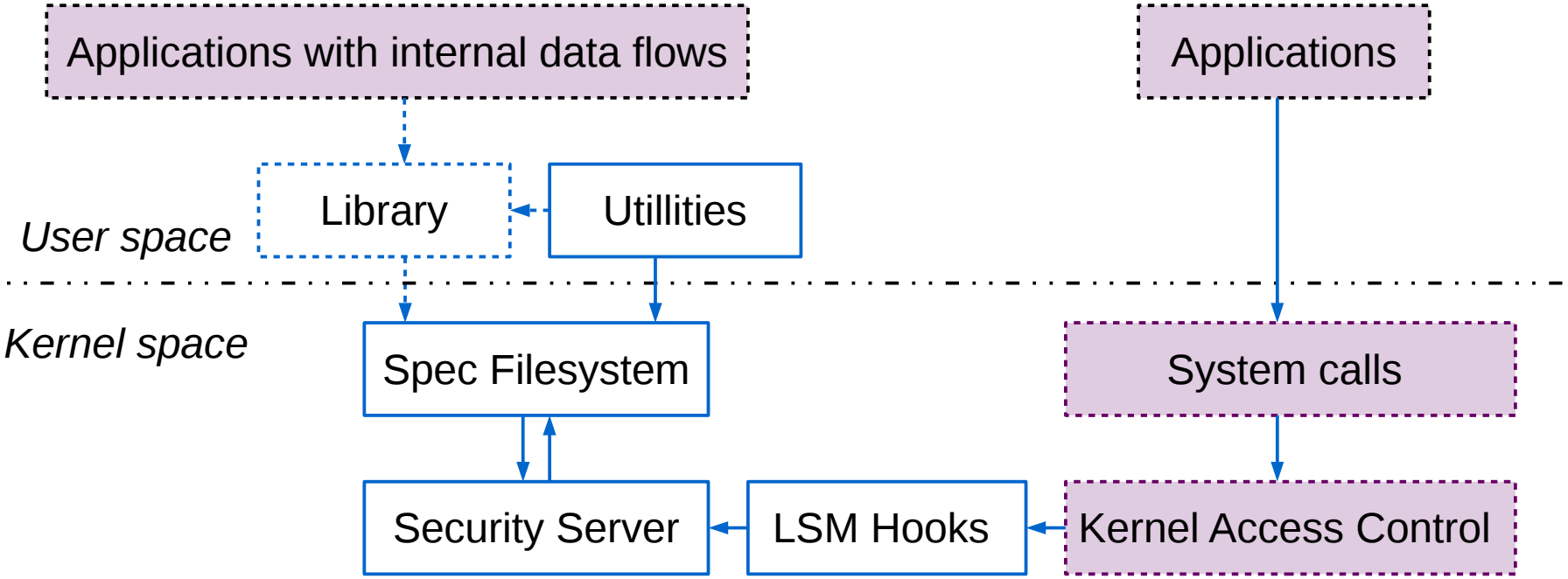
Функциональная спецификация ОС



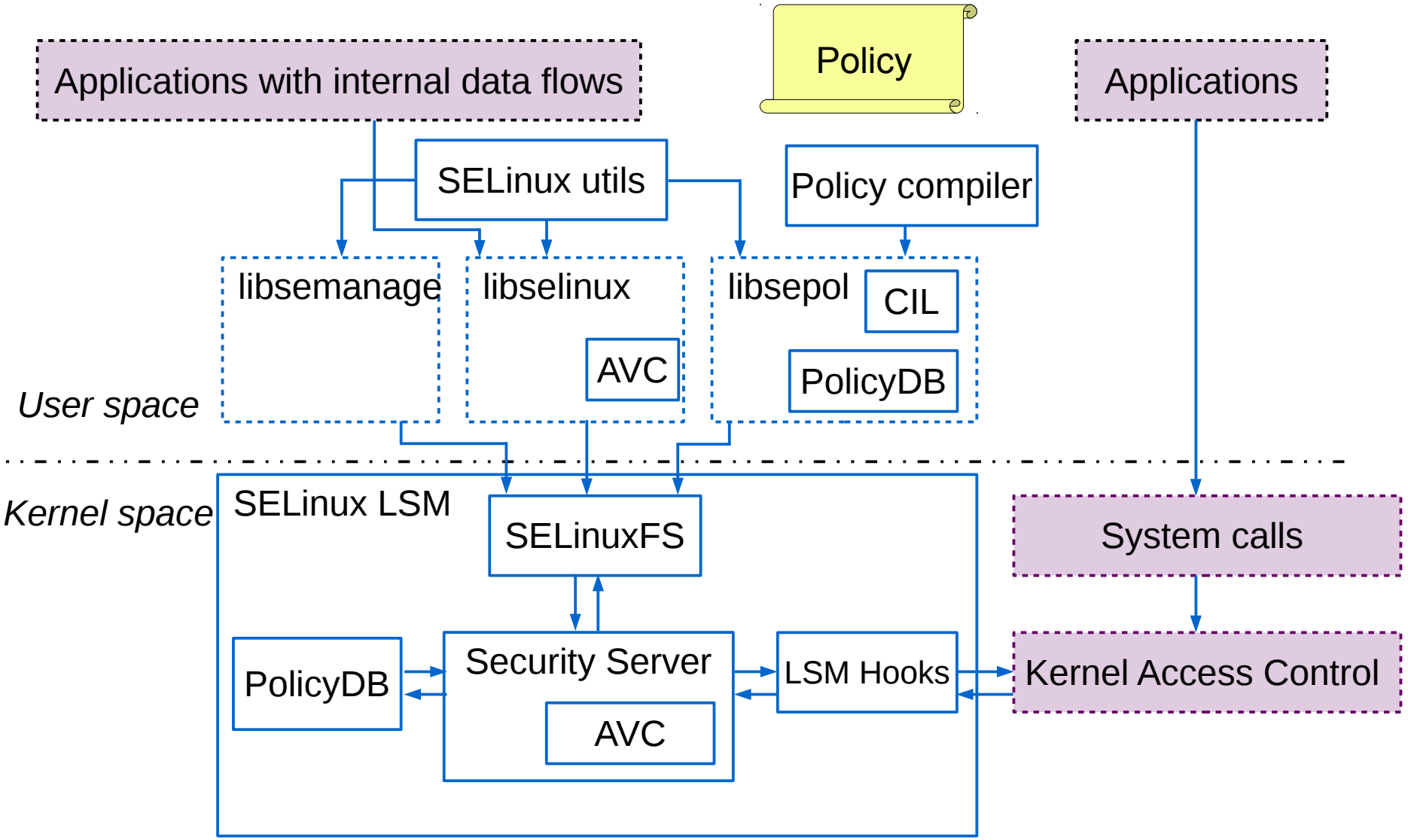
Функциональная спецификация ОС



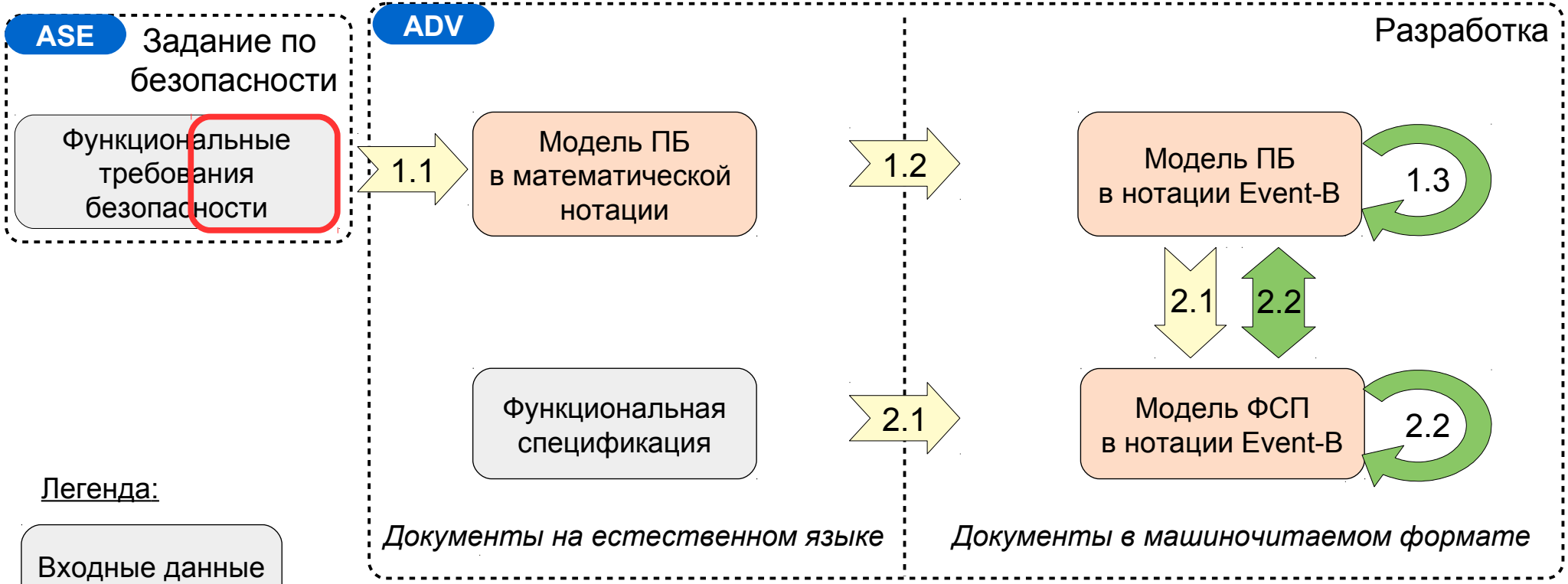
Компоненты parsec



Компоненты SELinux



Процесс моделирования и верификации ПБ



- 1. Моделирование ПБ
  - 1.1 Разработка модели ПБ в математической нотации
  - 1.2 Описание модели ПБ в нотации Event-B
  - 1.3 Верификация модели ПБ в нотации Event-B
- 2. Функциональная спецификация
  - 2.1 Формализация функциональной спецификации
  - 2.2 Верификация функциональной спецификации

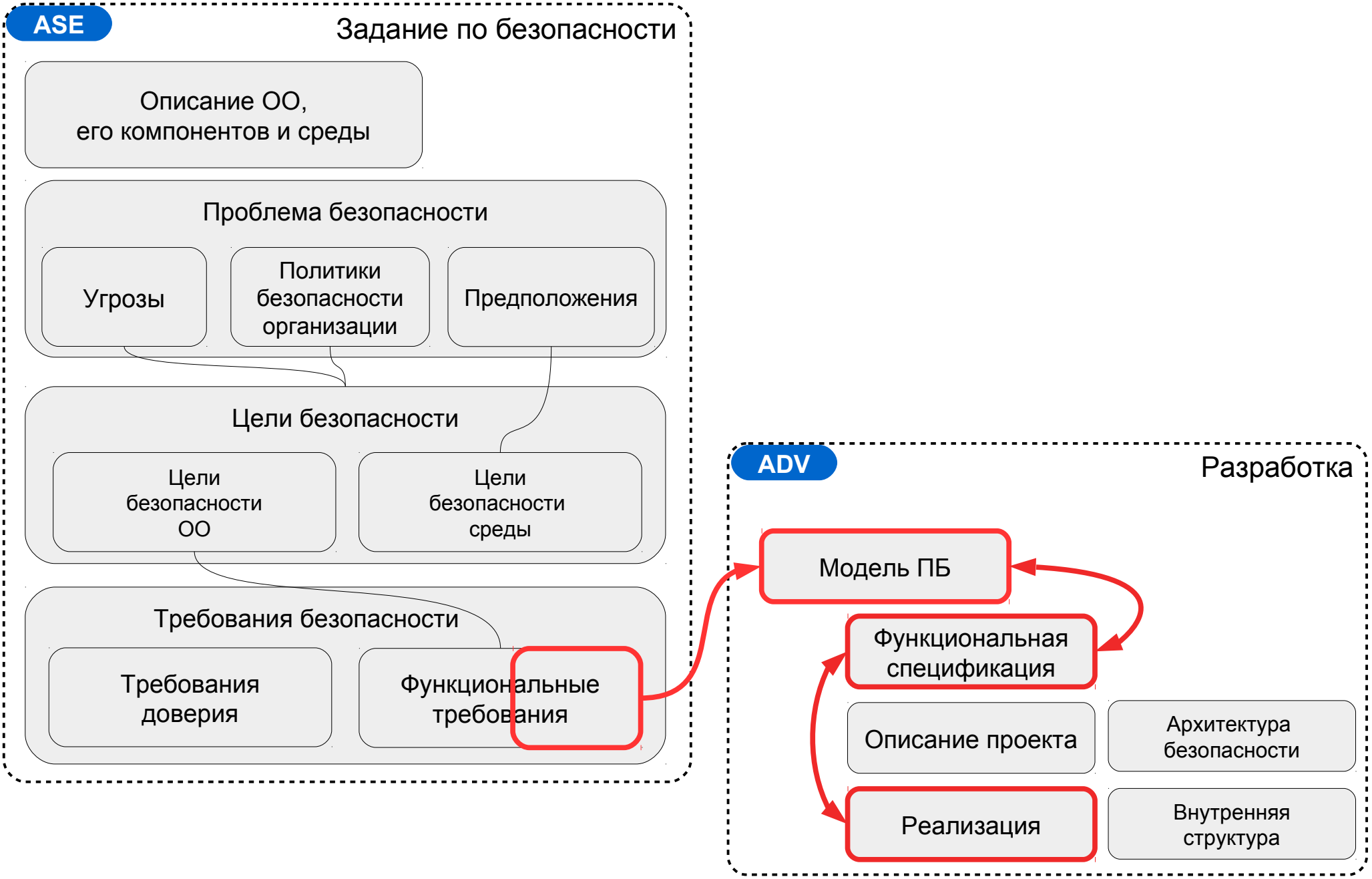
Процесс моделирования и верификации ПБ

- 1. Моделирование ПБ
  - 1.1 Разработка модели ПБ в математической нотации
  - 1.2 Описание модели ПБ в нотации Event-B
  - 1.3 Верификация модели ПБ в нотации Event-B
- 2. Функциональная спецификация
  - 2.1 Формализация функциональной спецификации
  - 2.2 Верификация функциональной спецификации
- 3. Верификация реализации
  - 3.1 Дедуктивная верификация ключевых компонентов
    - 3.1.1 Выделение ключевых компонентов
    - 3.1.2 Спецификация требований к компоненту и его окружению
    - 3.1.3 Дедуктивная верификация компонентов
  - 3.2 Тестирование реализации
    - 3.2.1 Мониторинг соответствия модели ФСП

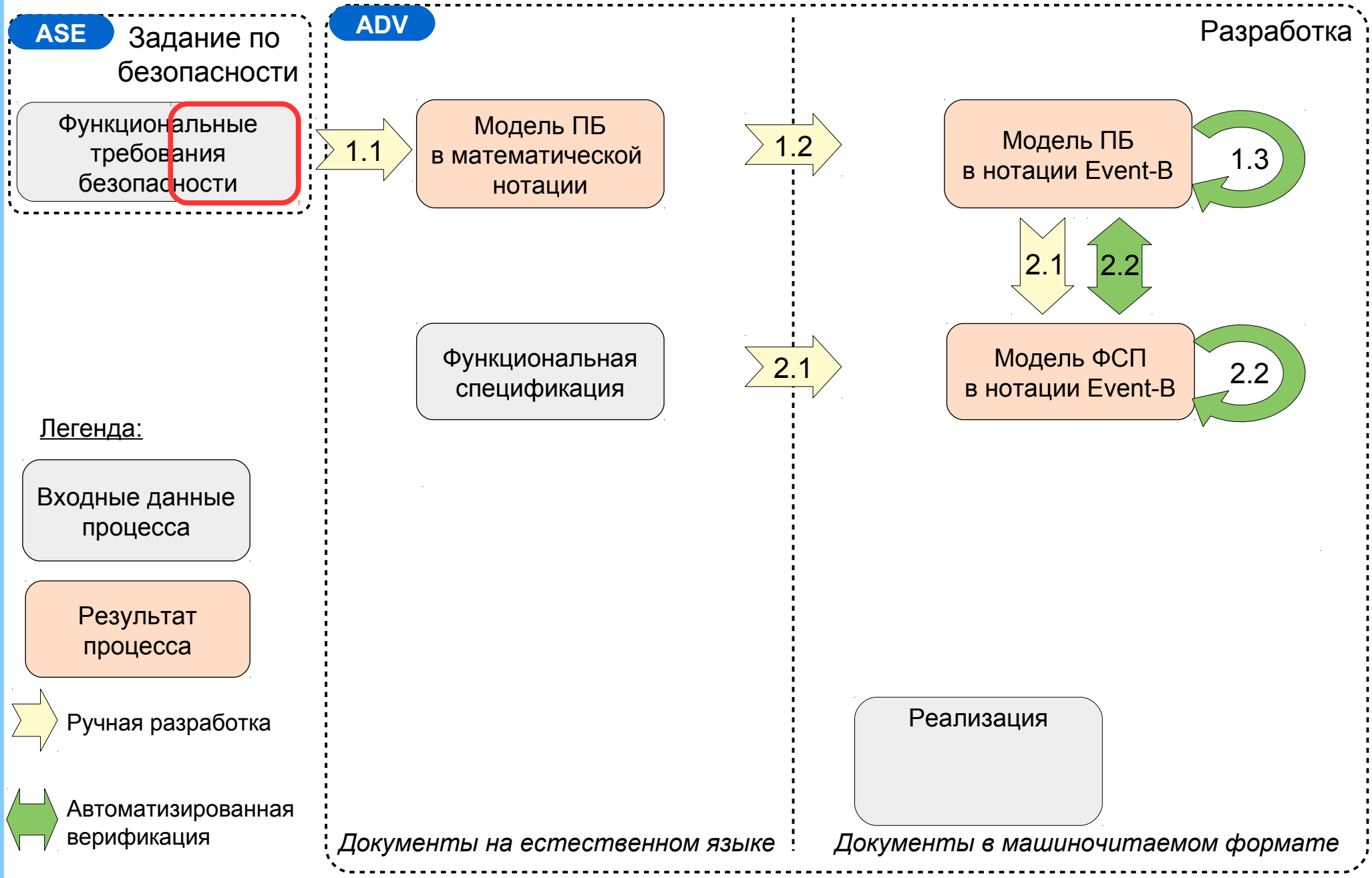
Процесс моделирования и верификации ПБ

- 1. Моделирование ПБ
  - 1.1 Разработка модели ПБ в математической нотации
  - 1.2 Описание модели ПБ в нотации Event-B
  - 1.3 Верификация модели ПБ в нотации Event-B
- 2. Функциональная спецификация
  - 2.1 Формализация функциональной спецификации
  - 2.2 Верификация функциональной спецификации
- 3. Верификация реализации
  - 3.1 Дедуктивная верификация ключевых компонентов
    - 3.1.1 Выделение ключевых компонентов
    - 3.1.2 Спецификация требований к компоненту и его окружению
    - 3.1.3 Дедуктивная верификация компонентов
  - 3.2 Тестирование реализации
    - 3.2.1 Мониторинг соответствия модели ФСП

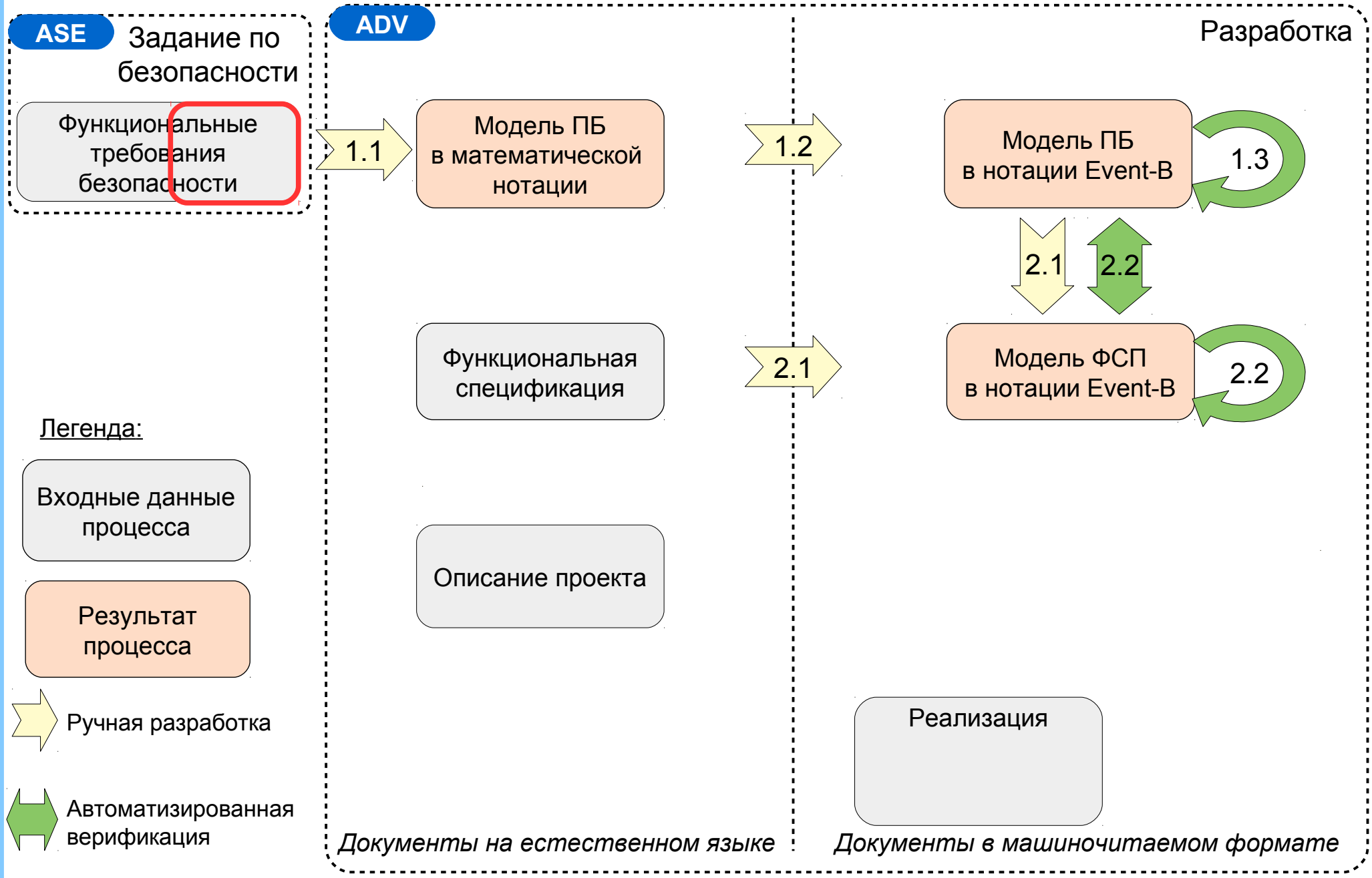
ГОСТ Р 15408-3-2013 Критерии оценки безопасности ИТ



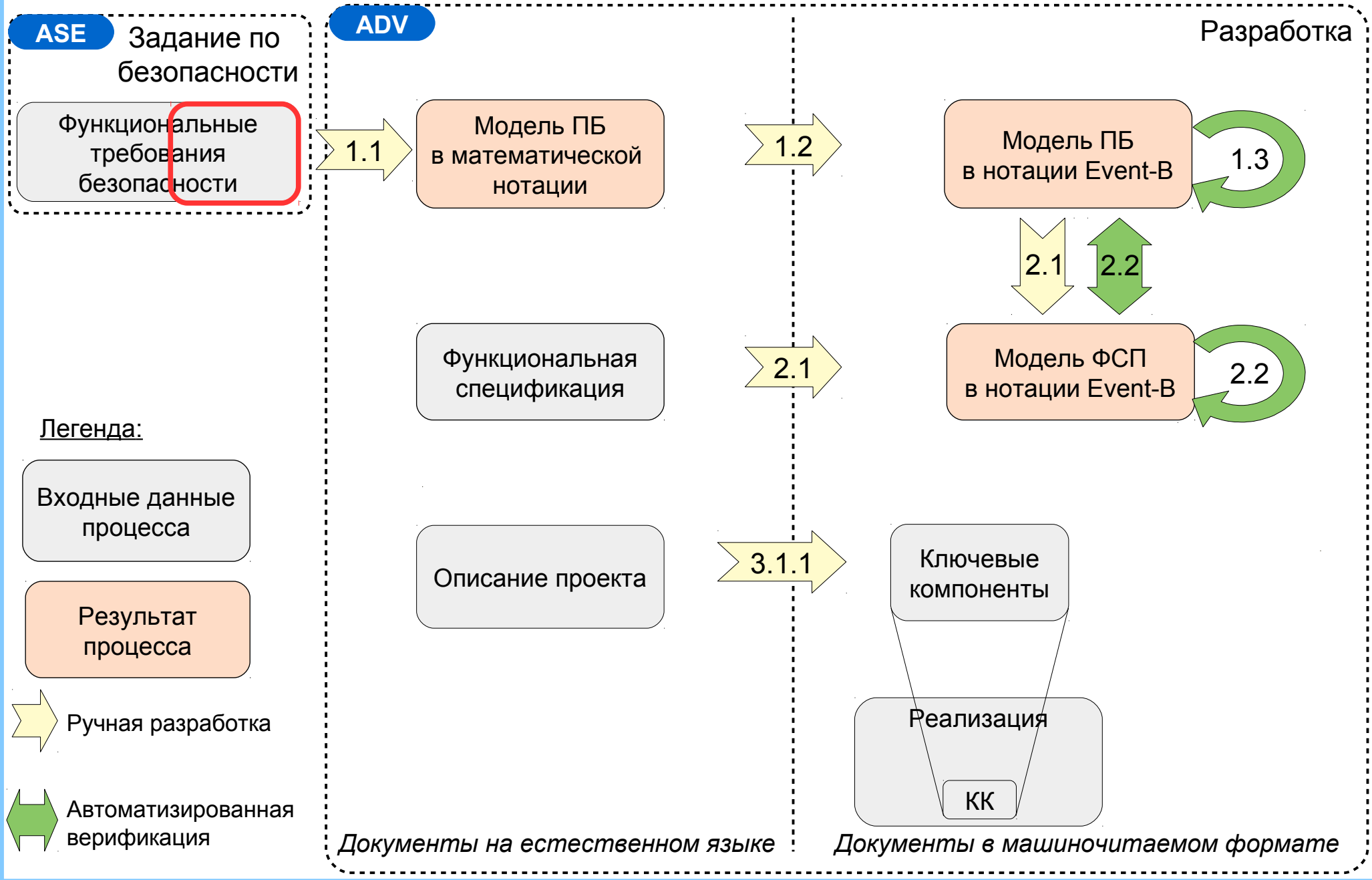
Процесс моделирования и верификации ПБ



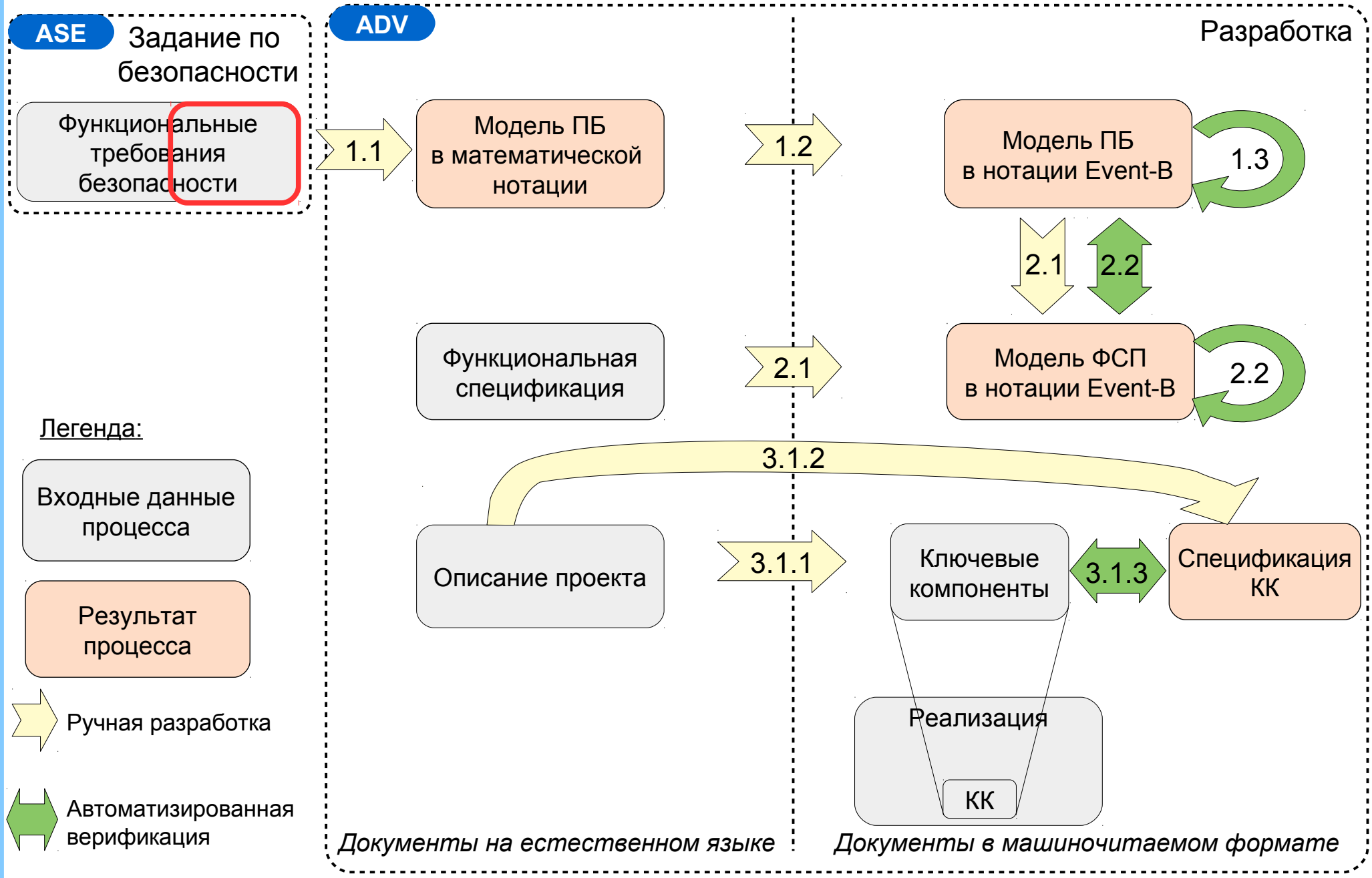
Процесс моделирования и верификации ПБ



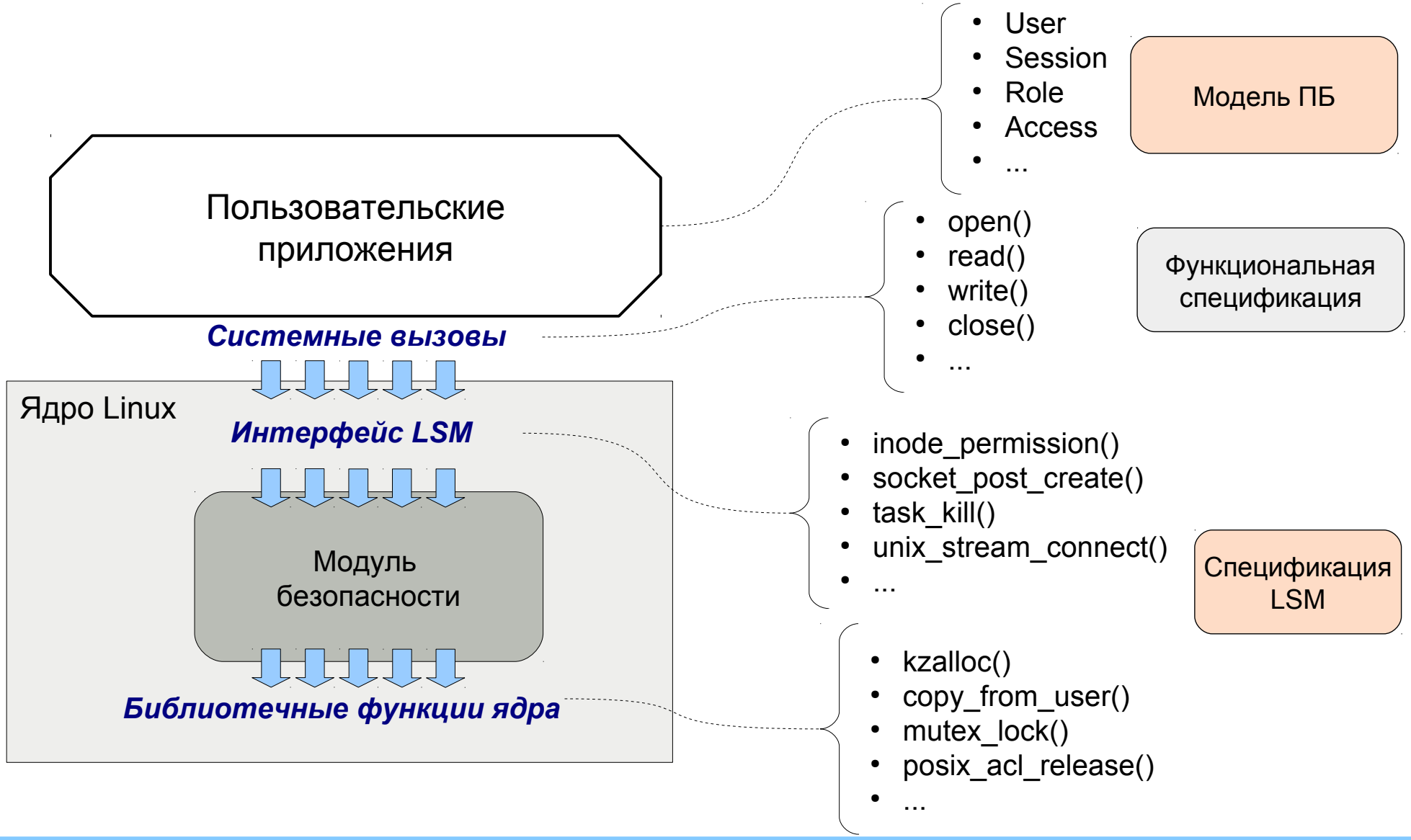
Процесс моделирования и верификации ПБ



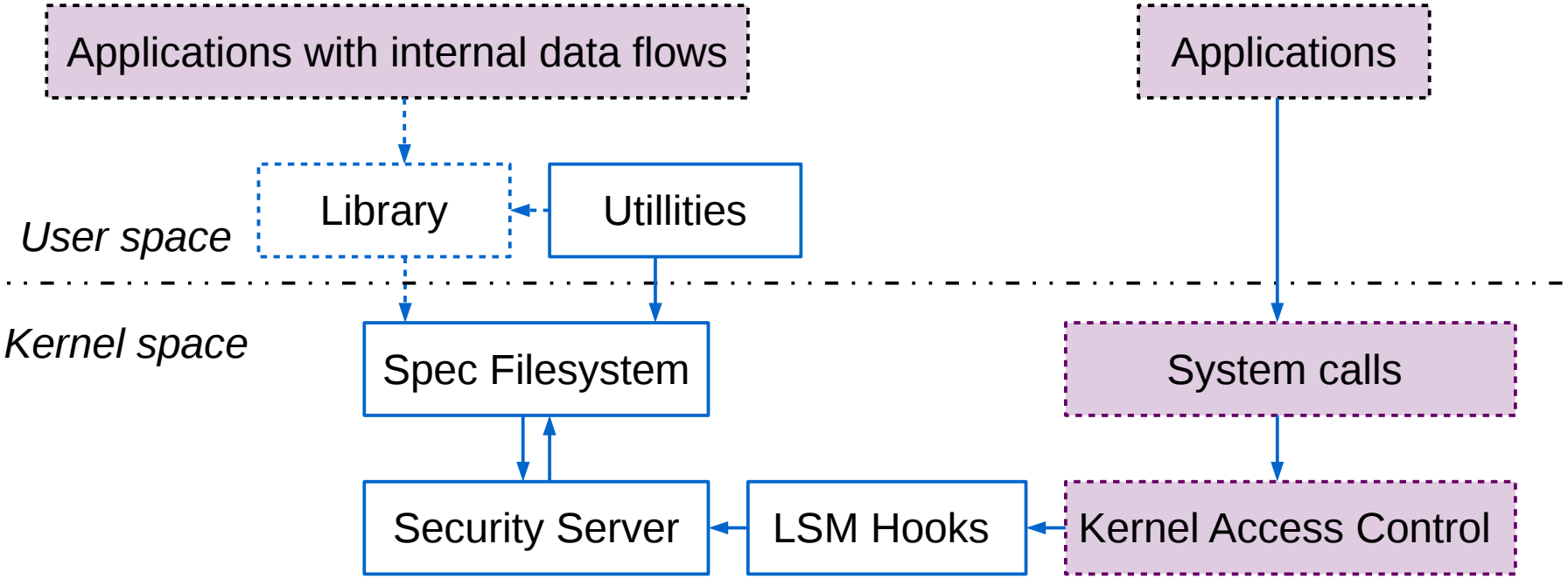
Процесс моделирования и верификации ПБ



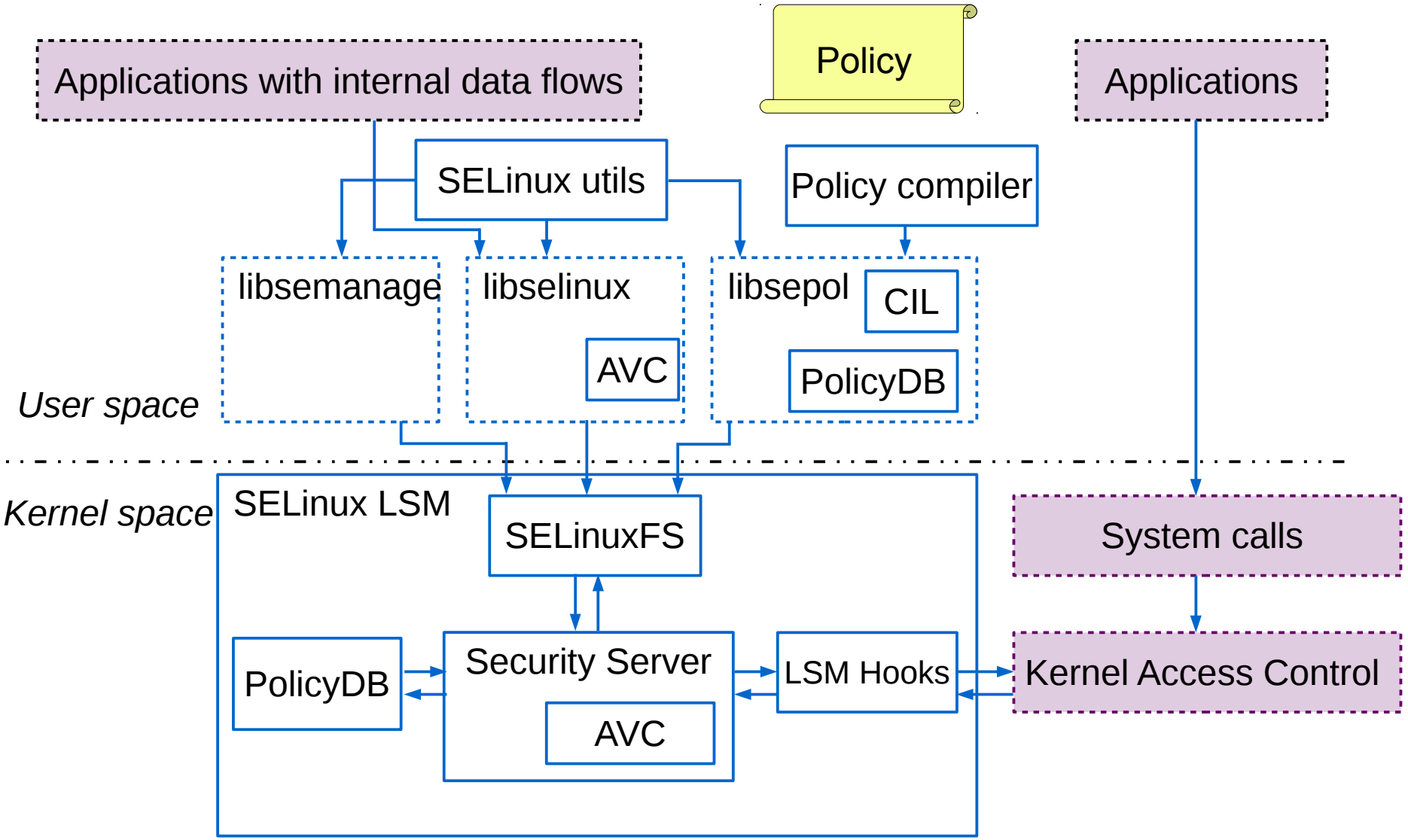
Спецификация LSM



Компоненты parsec



Компоненты SELinux



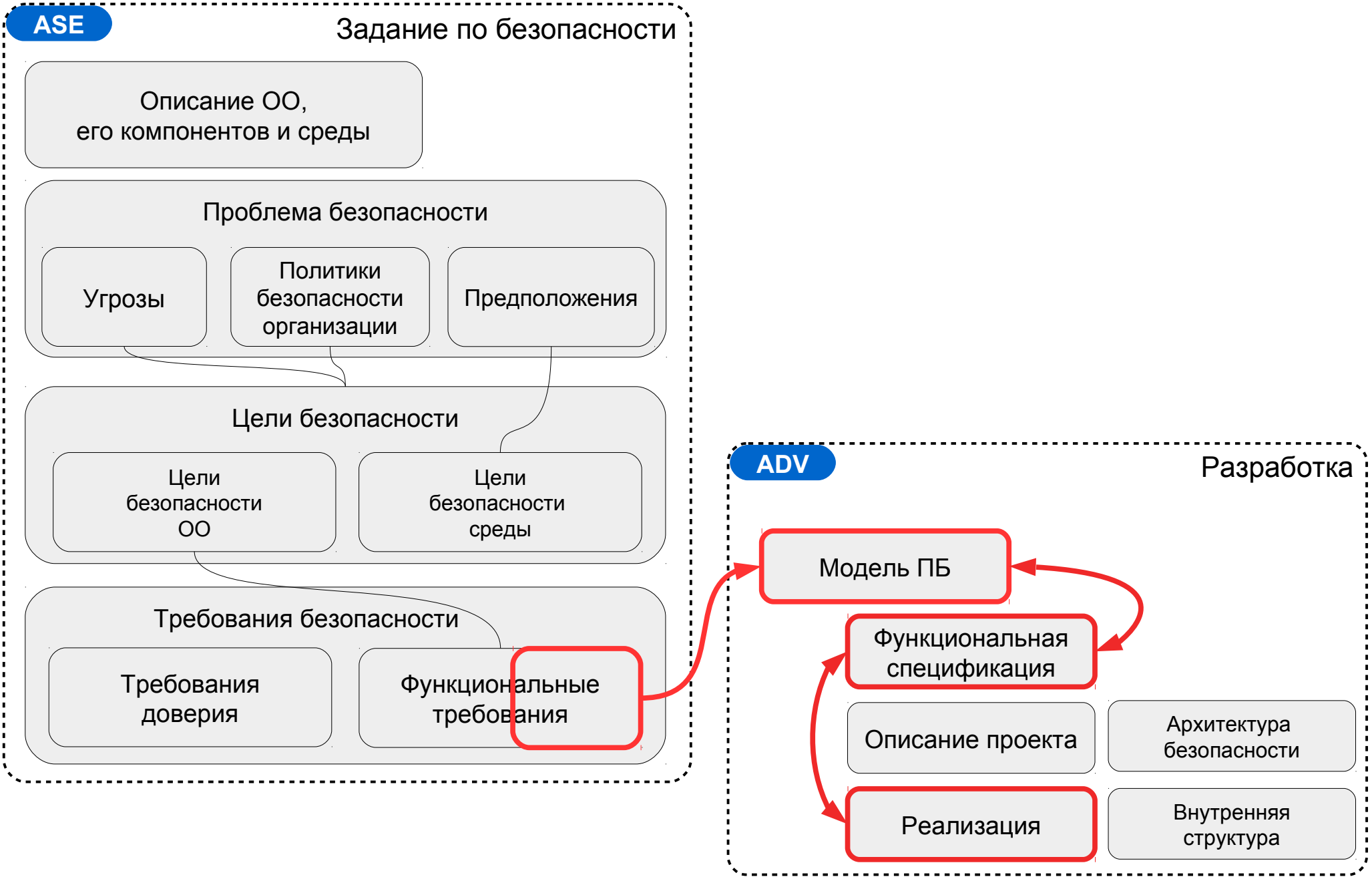
Процесс моделирования и верификации ПБ

- 1. Моделирование ПБ
  - 1.1 Разработка модели ПБ в математической нотации
  - 1.2 Описание модели ПБ в нотации Event-B
  - 1.3 Верификация модели ПБ в нотации Event-B
- 2. Функциональная спецификация
  - 2.1 Формализация функциональной спецификации
  - 2.2 Верификация функциональной спецификации
- 3. Верификация реализации
  - 3.1 Дедуктивная верификация ключевых компонентов
    - 3.1.1 Выделение ключевых компонентов
    - 3.1.2 Спецификация требований к компоненту и его окружению
    - 3.1.3 Дедуктивная верификация компонентов
  - 3.2 Тестирование реализации
    - 3.2.1 Мониторинг соответствия модели ФСП

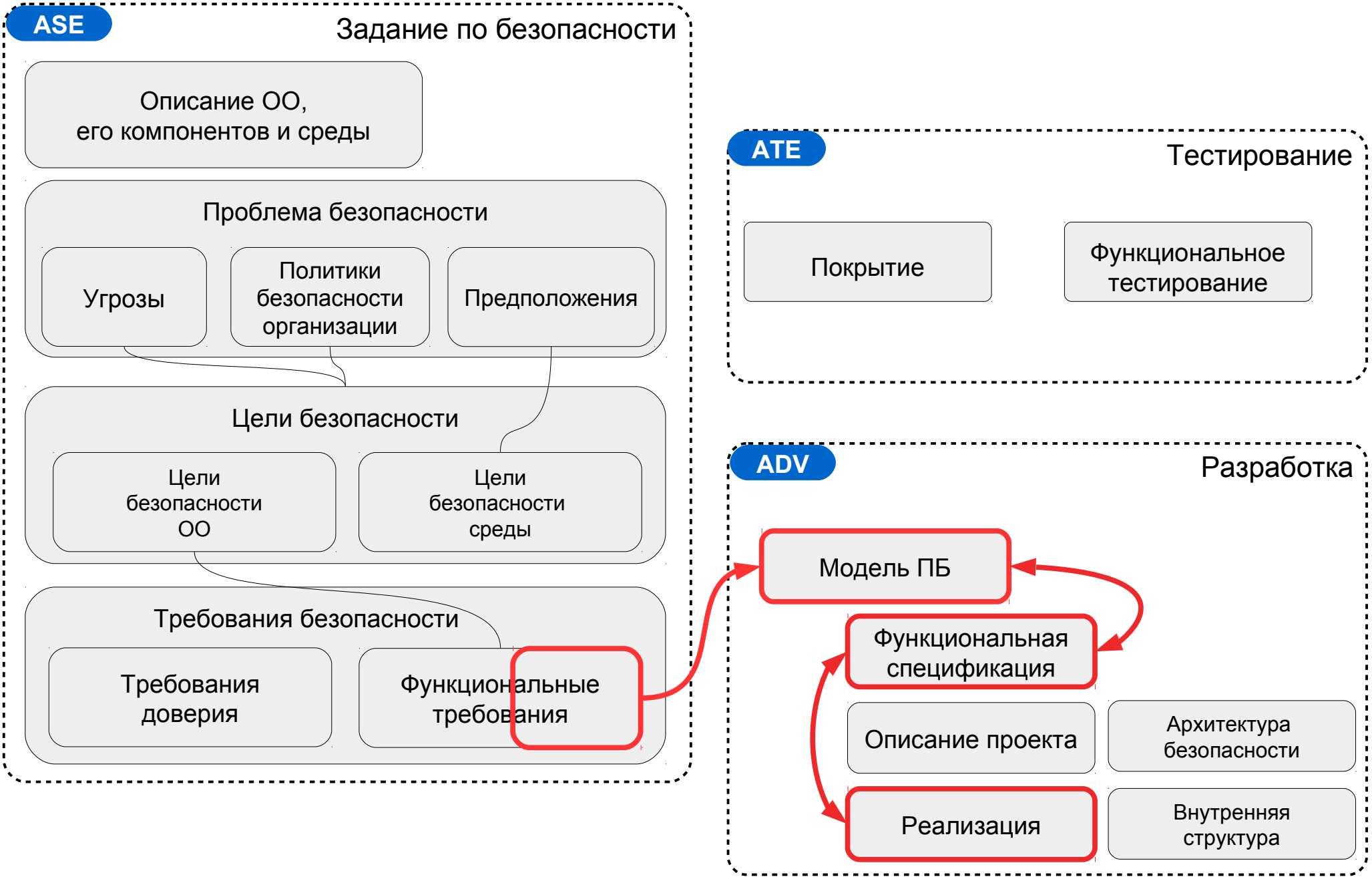
Процесс моделирования и верификации ПБ

- 1. Моделирование ПБ
  - 1.1 Разработка модели ПБ в математической нотации
  - 1.2 Описание модели ПБ в нотации Event-B
  - 1.3 Верификация модели ПБ в нотации Event-B
- 2. Функциональная спецификация
  - 2.1 Формализация функциональной спецификации
  - 2.2 Верификация функциональной спецификации
- 3. Верификация реализации
  - 3.1 Дедуктивная верификация ключевых компонентов
    - 3.1.1 Выделение ключевых компонентов
    - 3.1.2 Спецификация требований к компоненту и его окружению
    - 3.1.3 Дедуктивная верификация компонентов
  - 3.2 Тестирование реализации
    - 3.2.1 Мониторинг соответствия модели ФСП

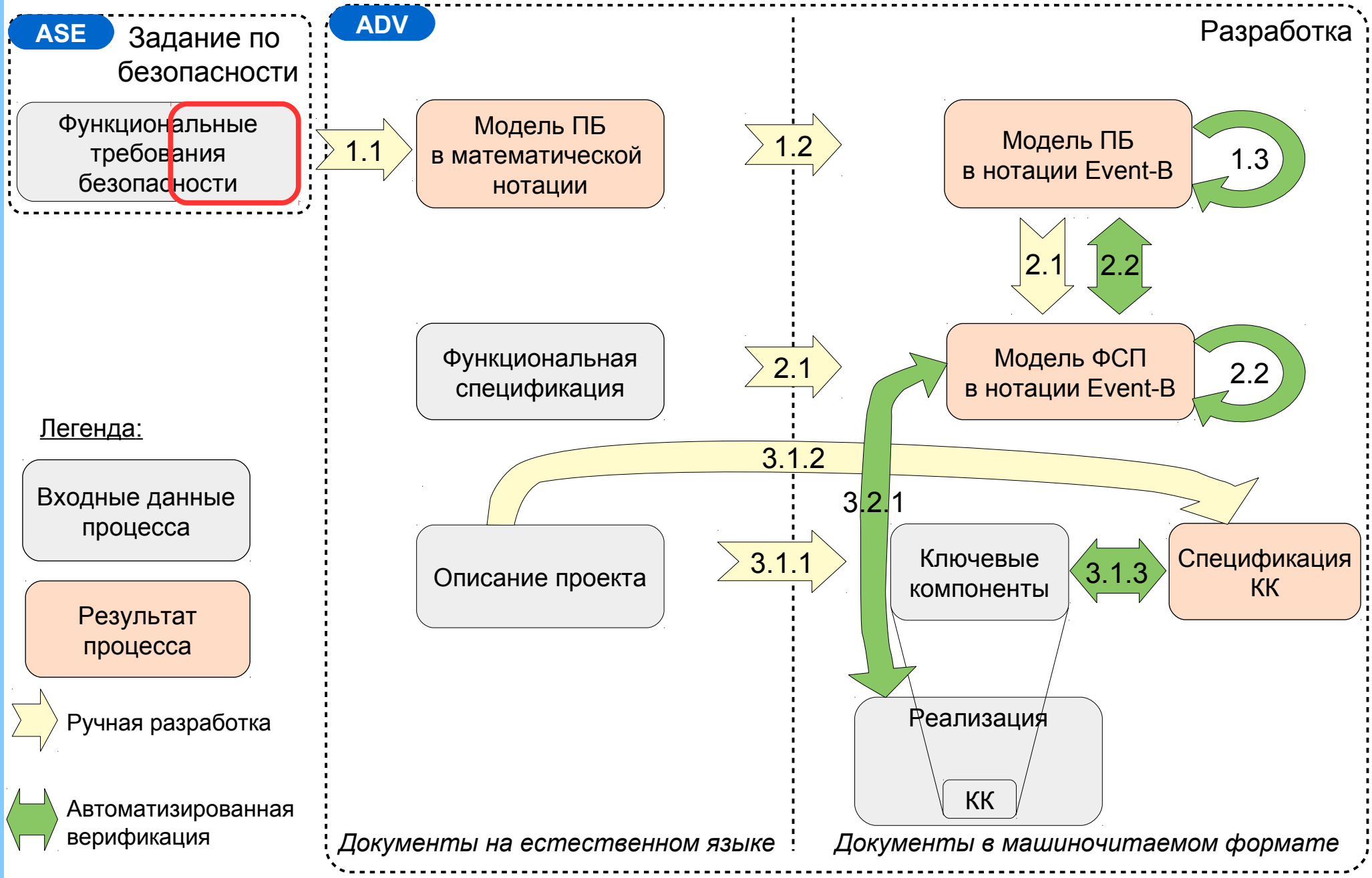
ГОСТ Р 15408-3-2013 Критерии оценки безопасности ИТ



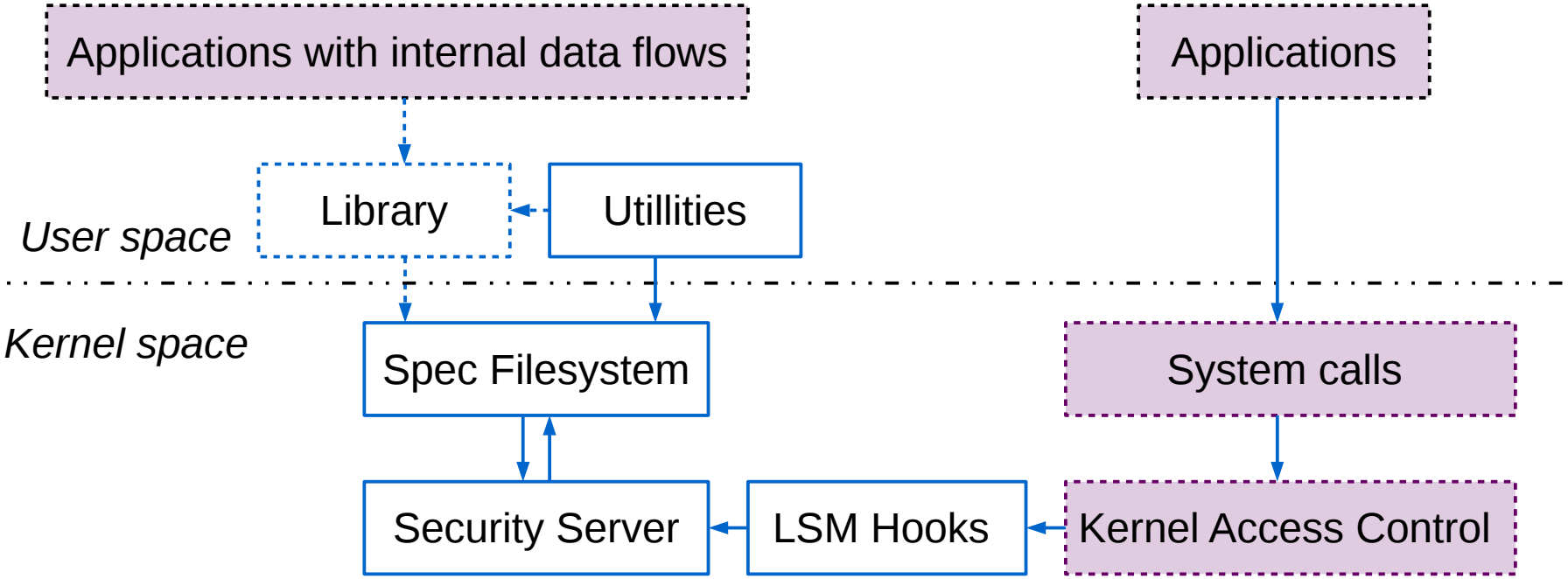
ГОСТ Р 15408-3-2013 Критерии оценки безопасности ИТ



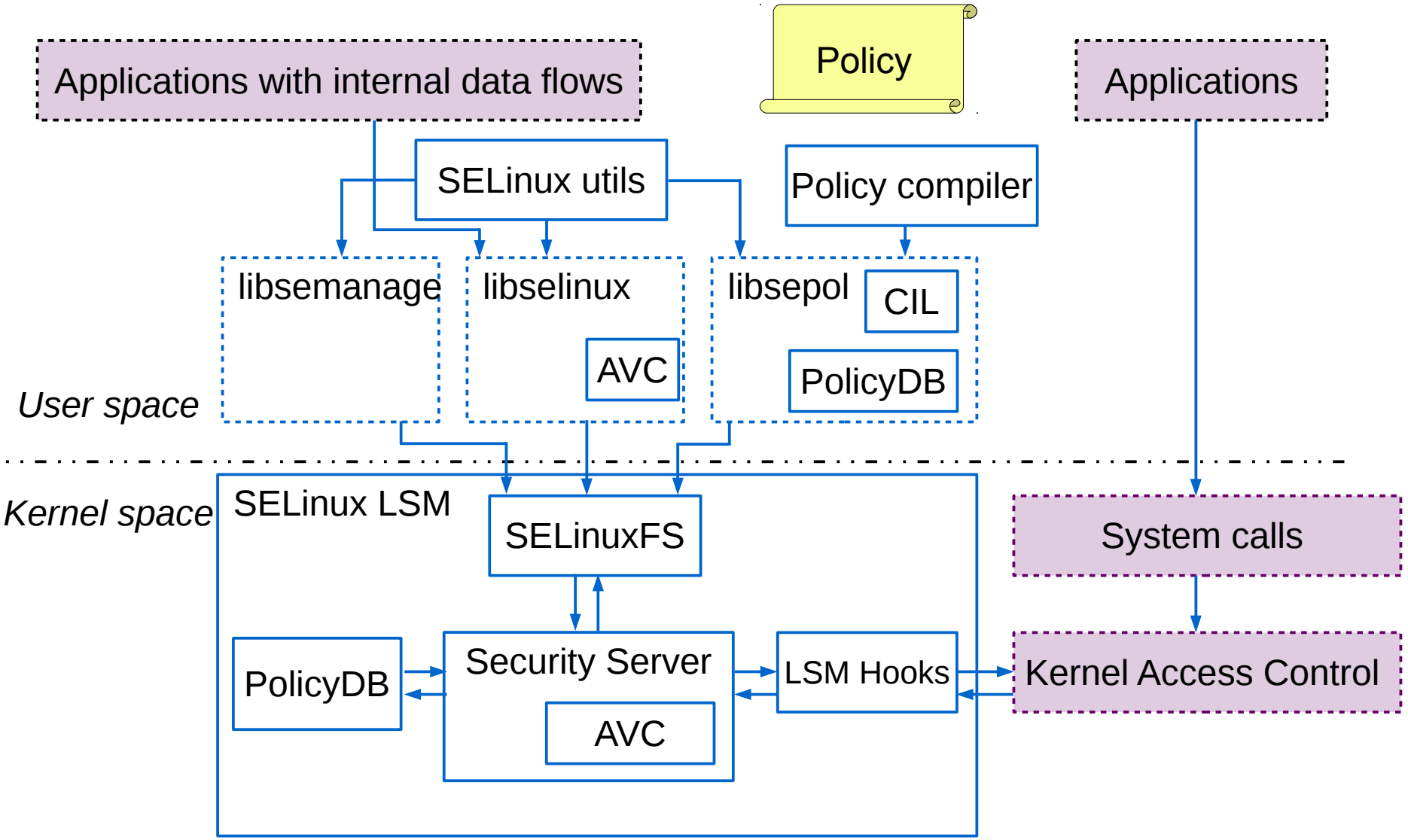
Процесс моделирования и верификации ПБ



Компоненты parsec



Компоненты SELinux



Процесс моделирования и верификации ПБ

- 1. Моделирование ПБ
  - 1.1 Разработка модели ПБ в математической нотации
  - 1.2 Описание модели ПБ в нотации Event-B
  - 1.3 Верификация модели ПБ в нотации Event-B
- 2. Функциональная спецификация
  - 2.1 Формализация функциональной спецификации
  - 2.2 Верификация функциональной спецификации
- 3. Верификация реализации
  - 3.1 Дедуктивная верификация ключевых компонентов
    - 3.1.1 Выделение ключевых компонентов
    - 3.1.2 Спецификация требований к компоненту и его окружению
    - 3.1.3 Дедуктивная верификация компонентов
  - 3.2 Тестирование реализации
    - 3.2.1 Мониторинг соответствия модели ФСП

Спасибо!