

Оглавление

Предисловие	3
1. Формальные методы в разработке и сертификации средств защиты информации	6
2. Описание процесса моделирования и верификации механизма управления доступом операционной системы	12
2.1. Этап I. Формализация модели политики безопасности управления доступом и ее верификация	14
2.2. Этап II. Разработка спецификации системных вызовов ОС и доказательство ее соответствия с формальной моделью политики безопасности	16
2.3. Этапы III и IV. Исследование механизма управления доступом ОС	17
2.4. Замечание об используемой терминологии	22
3. Модель политики безопасности управления доступом — требования к составу и структуре модели. Базовый уровень МРОСЛ ДП-модели	25
3.1. Требования к составу и структуре модели	25
3.2. Базовый уровень МРОСЛ ДП-модели в математической нотации	33
3.3. Состояние системы: структуры данных модели	40
3.3.1. Элементы состояния системы	40
3.3.2. Условия консистентности модели	48
3.3.3. Де-юре правила перехода системы из состояния в состояние	56
3.3.4. Обоснование выполнения условий консистентности модели	72
4. Event-B спецификация базового уровня МРОСЛ ДП-модели	80
4.1. Формальные спецификации	80
4.2. Связь элементов МРОСЛ ДП-модели и элементов спецификации Event-B	83
4.3. Контекст	84
4.4. Машина	87
4.4.1. Переменные и инварианты	87
4.4.2. Событие инициализации	98

4.4.3. Реализация правила перехода системы из состояния в состояние в виде события	98
4.4.4. Использование вспомогательных параметров	100
4.4.5. Использование математической индукции	103
4.4.6. Разделение правила перехода системы из состояния в состояние на несколько событий	106
4.4.7. Отсутствующие в спецификации элементы МРОСЛ ДП-модели	108
4.4.8. Формализация свойств безопасности МРОСЛ ДП-модели	108
4.5. Верификация	109
4.6. Использование уточнения	111
5. Формальная функциональная спецификация	114
5.1. Построение соответствия между системными вызовами и правилами МРОСЛ ДП-модели	118
5.2. Пример формализации функциональной спецификации	121
6. Дедуктивная верификация модуля безопасности ядра ОС Linux	125
6.1. Подсистема LSM. Функционирование модуля безопасности ядра ОС Linux	126
6.2. Дедуктивная верификация кода на языке Си	132
6.2.1. Инструментарий	134
6.2.2. Пример спецификаций на языке ACSL	137
6.2.3. Текущие ограничения стека инструментов Frama-C/AstraVer	144
6.3. Процесс верификации: работы, планирование, координация	144
6.4. Согласование правил разработки кода	145
6.4.1. Работа с макросами	146
6.4.2. Разработка спецификаций	147
6.4.3. Планирование работ. Оценка сложности	147
6.4.4. Разработка спецификаций для функций ядра, которые использует модуль безопасности	149
6.4.5. Тактика верификации — рабочий цикл процесса	150
6.5. Пример	151
7. Динамический мониторинг	169
7.1. Управление доступом в ядре ОС Linux	169
7.2. Схема работы анализа	171
7.3. Сбор трасс ядра	175
7.4. Механизм воспроизведения трасс на Event-B спецификации	176

7.5. Интеграция дедуктивной верификации и динамического мониторинга при верификации модуля безопасности	180
Заключение.....	183
Используемые сокращения и обозначения.....	184
Литература.....	185
Приложения.....	191
Приложение А. Язык спецификаций Event-B.....	191
Приложение В. Среда разработки и верификации на языке Event-B.....	209