

Оглавление

Предисловие

Предисловие ко второму изданию

Глава 1. Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем

- 1.1. Элементы теории компьютерной безопасности
 - 1.1.1. Сущность, субъект, доступ, информационный поток
 - 1.1.2. Классическая классификация угроз безопасности информации
 - 1.1.3. Виды информационных потоков
 - 1.1.4. Виды политик управления доступом и информационными потоками
 - 1.1.5. Утечка права доступа и нарушение безопасности КС
- 1.2. Математические основы моделей безопасности
 - 1.2.1. Основные понятия
 - 1.2.2. Понятие автомата
 - 1.2.3. Элементы теории графов
 - 1.2.4. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы
 - 1.2.5. Модель решетки
- 1.3. Основные виды формальных моделей безопасности
- 1.4. Проблема адекватности реализации модели безопасности в реальной компьютерной системе
- 1.5. Контрольные вопросы и задачи

Глава 2. Модели компьютерных систем с дискреционным управлением доступом

- 2.1. Модель матрицы доступов Харрисона–Руззо–Ульмана
 - 2.1.1. Описание модели
 - 2.1.2. Анализ безопасности систем ХРУ
 - 2.1.3. Модель типизированной матрицы доступов
- 2.2. Модель распространения прав доступа Take-Grant
 - 2.2.1. Основные положения классической модели Take-Grant
 - 2.2.2. Расширенная модель Take-Grant
 - 2.2.3. Представление систем Take-Grant системами ХРУ
- 2.3. Дискреционные ДП-модели
 - 2.3.1. Базовая ДП-модель
 - 2.3.2. ДП-модель без кооперации доверенных и недоверенных субъектов
- 2.4. Контрольные вопросы и задачи

Глава 3. Модели изолированной программной среды

- 3.1. Субъектно-ориентированная модель изолированной программной среды
- 3.2. Корректность субъектов в ДП-моделях КС с дискреционным управлением доступом
 - 3.2.1. ДП-модель с функционально ассоциированными с субъектами сущностями
 - 3.2.2. ДП-модель для политики безопасного администрирования
 - 3.2.3. ДП-модель для политики абсолютного разделения административных и пользовательских полномочий
 - 3.2.4. ДП-модель с функционально или параметрически ассоциированными с субъектами сущностями
 - 3.2.5. Применение ФАС ДП-модели для анализа безопасности веб-систем
- 3.3. Методы предотвращения утечки прав доступа и реализации запрещенных информационных потоков
 - 3.3.1. Метод предотвращения возможности получения права доступа владения недоверенным субъектом к доверенному субъекту
 - 3.3.2. Метод реализации политики безопасного администрирования
 - 3.3.3. Метод реализации политики абсолютного разделения административных и пользовательских полномочий
- 3.4. Контрольные вопросы и задачи

Глава 4. Модели компьютерных систем с мандатным управлением доступом

- 4.1. Модель Белла–ЛаПадулы
 - 4.1.1. Классическая модель Белла–ЛаПадулы

- 4.1.2. Пример некорректного определения свойств безопасности
- 4.1.3. Политика low-watermark в модели Белла–ЛаПадулы
- 4.1.4. Примеры реализации запрещенных информационных потоков
- 4.1.5. Безопасность переходов
- 4.1.6. Модель мандатной политики целостности информации Биба
- 4.2. Модель систем военных сообщений
- 4.2.1. Общие положения и основные понятия
- 4.2.2. Неформальное описание модели СВС
- 4.2.3. Формальное описание модели СВС
- 4.3. Мандатная ДП-модель
- 4.3.1. Правила преобразования состояний мандатной ДП-модели
- 4.3.2. Безопасность в смысле Белла–ЛаПадулы
- 4.3.3. Условия повышения субъектом уровня доступа
- 4.4. Контрольные вопросы и задачи

Глава 5. Модели безопасности информационных потоков

- 5.1. Автоматная модель безопасности информационных потоков
- 5.2. Программная модель контроля информационных потоков
- 5.3. Вероятностная модель безопасности информационных потоков
- 5.4. ДП-модели безопасности информационных потоков по времени
- 5.4.1. ДП-модель с блокирующими доступами доверенных субъектов
- 5.4.2. Мандатная ДП-модель с блокирующими доступами доверенных субъектов
- 5.4.3. Мандатная ДП-модель с отождествлением порожденных субъектов
- 5.4.4. Мандатная ДП-модель КС, реализующих политику строгого мандатного управления доступом
- 5.5. Контрольные вопросы и задачи

Глава 6. Модели компьютерных систем с ролевым управлением доступом

- 6.1. Понятие ролевого управления доступом
- 6.2. Базовая модель ролевого управления доступом
- 6.3. Модель администрирования ролевого управления доступом
- 6.3.1. Основные положения
- 6.3.2. Администрирование множеств авторизованных ролей пользователей
- 6.3.3. Администрирование множеств прав доступа
- 6.3.4. Администрирование иерархии ролей
- 6.4. Модель мандатного ролевого управления доступом
- 6.4.1. Защита от угрозы конфиденциальности информации
- 6.4.2. Защита от угроз конфиденциальности и целостности информации
- 6.5. Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux
- 6.5.1. Состояние системы
- 6.5.2. Функционально или параметрически ассоциированные сущности
- 6.5.3. Доступы и права доступа
- 6.5.4. Задание мандатного управления доступом для состояний системы
- 6.5.5. Задание мандатного контроля целостности для состояний системы
- 6.5.6. Фактическое владение
- 6.5.7. Правила преобразования состояний
- 6.6. Контрольные вопросы и задачи

Приложение 1. Методические рекомендации по организации изучения моделей безопасности компьютерных систем

Анализ требований ФГОС ВПО

Организация изучения моделей безопасности КС

Приложение 2. Примеры решения задач на практических занятиях

Практическое занятие № 1. Модель решетки

Практическое занятие № 2. Модели ХРУ и ТМД

Практическое занятие № 3. Классическая модель Take-Grant

Практическое занятие № 4. Расширенная модель Take-Grant

Практическое занятие № 5. Классическая модель Белла–ЛаПадулы и ее интерпретации

Практическое занятие № 6. Модель СВС

Практическое занятие № 7. Модели безопасности информационных потоков

Практическое занятие № 8. Модели ролевого управления доступом

Практическое занятие № 9. Дискреционные ДП-модели

Практическое занятие № 10. Мандатные и ролевые ДП-модели

Список литературы