

Оглавление

Предисловие.....	3
1 Понятие защищенной операционной системы.....	4
1.1. Основные определения.....	4
1.2. Основные подходы к построению защищенных опера- ционных систем.....	4
1.3. Административные меры защиты.....	6
1.4. Адекватная политика безопасности.....	6
1.5. Стандарты безопасности операционных систем.....	10
Вопросы для самопроверки.....	15
2 Управление доступом.....	14
2.1. Основные определения.....	14
2.2. Типовые модели управления доступом.....	19
2.3. Управление доступом в Windows.....	26
2.4. Управление доступом в UNIX.....	62
Вопросы для самопроверки.....	69
3 Аутентификация.....	72
3.1. Общие сведения.....	72
3.2. Аутентификация в UNIX.....	92
3.3. Аутентификация в Windows.....	99
Вопросы для самопроверки.....	108
4 Аудит и обнаружение вторжений.....	110
4.1. Общие сведения.....	110
4.2. Системы обнаружения вторжений.....	114
4.3. Аудит в Windows.....	120
4.4. Аудит в UNIX.....	124
Вопросы для самопроверки.....	132
5 Домены Windows.....	134
5.1. Общие сведения.....	134
5.2. Сквозная аутентификация.....	135
5.3. Отношения доверия.....	139
5.4. Активный каталог.....	141
5.5. Групповая политика.....	149
Вопросы для самопроверки.....	155

6	Безопасность операционных систем мобильных устройств	157
	Вопросы для самопроверки	165
7	Виртуализация операционных систем	169
	Вопросы для самопроверки	180
	Приложение. Методические рекомендации по организации изучения дисциплины «Защита в операционных системах»	182
	Анализ требований ФГОС ВПО	182
	Организация изучения дисциплины «Защита в операционных системах»	186
	Литература	189