

БЕЗОПАСНОСТЬ

операционной системы
специального назначения

Astra Linux Special Edition

версия 1.6



СДЕЛАНО
В
РОССИИ



Оглавление

Предисловие	3
Глава 1. Обеспечение безопасности операционных систем семейства Linux	7
1.1. Понятие защищённой (доверенной) операционной системы.....	7
1.2. Обзор защищённых операционных систем семейства Linux	9
1.3. Архитектура, назначение и области применения ОССН	18
1.3.1. Назначение ОССН.....	18
1.3.2. Архитектура ОССН	23
1.3.3. Области применения ОССН	51
1.4. Основы пользовательской работы и администрирования в ОССН.....	55
1.4.1. Варианты загрузки, экраны входа и выхода из ОССН	55
1.4.2. Основные приёмы работы с защищённой графической подсистемой <i>Fly</i>	64
1.4.3. Основные задачи администрирования ОССН	68
Контрольные вопросы.....	88
Глава 2. Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux	90
2.1. Подход к формированию модели в её иерархическом представлении	90
2.2. Уровень ролевого управления доступом	97
2.2.1. Элементы состояния системы	97
2.2.2. Условия корректности состояний и переходов между ними	104
2.2.3. Де-юре правила преобразования состояний	116
2.2.4. Подход к моделированию ролевого управления доступом в СУБД PostgreSQL	137
2.3. Уровень мандатного контроля целостности	139
2.3.1. Элементы состояния системы	139

Оглавление

Предисловие	3
Глава 1. Обеспечение безопасности операционных систем семейства Linux	7
1.1. Понятие защищённой (доверенной) операционной системы	7
1.2. Обзор защищённых операционных систем семейства Linux	9
1.3. Архитектура, назначение и области применения ОССН	18
1.3.1. Назначение ОССН	18
1.3.2. Архитектура ОССН	23
1.3.3. Области применения ОССН	51
1.4. Основы пользовательской работы и администрирования в ОССН	55
1.4.1. Варианты загрузки, экраны входа и выхода из ОССН	55
1.4.2. Основные приёмы работы с защищённой графической подсистемой <i>Fly</i>	64
1.4.3. Основные задачи администрирования ОССН	68
Контрольные вопросы	88
Глава 2. Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux	90
2.1. Подход к формированию модели в её иерархическом представлении	90
2.2. Уровень ролевого управления доступом	97
2.2.1. Элементы состояния системы	97
2.2.2. Условия корректности состояний и переходов между ними	104
2.2.3. Де-юре правила преобразования состояний	116
2.2.4. Подходы к моделированию ролевого управления доступом в СУБД PostgreSQL	137
2.3. Уровень мандатного контроля целостности	139
2.3.1. Элементы состояния системы	139

2.3.2. Функционально или параметрически ассоциированные сущности	143
2.3.3. Условия корректности мандатного контроля целостности для состояний системы	146
2.3.4. Фактическое владение и де-факто правила преобразования состояний	159
2.3.5. Нарушение безопасности системы в смысле мандатного контроля целостности	165
2.4. Уровни мандатного управления доступом	171
2.4.1. Элементы состояния системы	171
2.4.2. Условия корректности мандатного управления доступом и правила преобразования состояний	173
2.4.3. Достаточные условия безопасности системы в смысле Велла-ЛаПадулы	180
2.4.4. Достаточные условия безопасности системы в смысле информационных потоков по времени	183
Контрольные вопросы	186
Глава 3. Управление безопасностью ОССН	188
3.1. Мандатное управление доступом	188
3.1.1. Проблемы реализации мандатного управления доступом в операционных системах	188
3.1.2. Реализация мандатного управления доступом в ОССН	192
3.1.3. Администрирование мандатного управления доступом в ОССН	199
3.2. Мандатный контроль целостности	211
3.3. Управление доступом к объектам графической подсистемы	216
3.4. Особенности аутентификации	220
3.5. Особенности аудита	234
3.6. Сетевое взаимодействие в ОССН. Организация доменной инфраструктуры	240
3.6.1. Логические уровни сетевой инфраструктуры	240
3.6.2. Формирование базового уровня сетевой инфраструктуры ОССН	241
3.6.3. Формирование корпоративного уровня сетевой инфраструктуры ОССН. Единое пространство пользователей	248
3.6.4. Служба ALD. Администрирование доменной сетевой инфраструктуры ОССН	257

3.6.5. Служба FreeIPA. Формирование гетерогенной доменной сетевой инфраструктуры	263
3.7. Дополнительные функции безопасности	272
Контрольные вопросы	280
Глава 4. Лабораторный практикум по администрированию ОССН	282
4.1. Лабораторная работа № 1. Работа с учётными записями пользователей и группами	282
Цель работы	282
Краткие теоретические сведения	282
Используемое методическое и лабораторное обеспечение	284
Порядок выполнения работы	286
Содержание отчёта о выполненной работе	293
Контрольные вопросы	293
4.2. Лабораторная работа № 2. Настройка параметров мандатного управления доступом и мандатного контроля целостности	293
Цель работы	293
Краткие теоретические сведения	293
Используемое методическое и лабораторное обеспечение	296
Порядок выполнения работы	296
Содержание отчёта о выполненной работе	304
Контрольные вопросы	305
4.3. Лабораторная работа № 3. Организация файловой системы ОССН для работы пользователей в рамках мандатного управления доступом и мандатного контроля целостности	305
Цель работы	305
Краткие теоретические сведения	306
Используемое методическое и лабораторное обеспечение	307
Порядок выполнения работы	307
Содержание отчёта о выполненной работе	314
Контрольные вопросы	315
4.4. Лабораторная работа № 4. Администрирование ОССН в рамках реализации мандатного контроля целостности	315
Цель работы	315

Краткие теоретические сведения	315
Используемое методическое и лабораторное обеспечение	316
Порядок выполнения работы	316
Содержание отчёта о выполненной работе	331
Контрольные вопросы	322
4.5. Лабораторная работа № 5. Настройка механизмов организации замкнутой программной среды. Контроль целостности КСЗ	322
Цель работы	322
Краткие теоретические сведения	322
Используемое методическое и лабораторное обеспечение	331
Порядок выполнения работы	331
Содержание отчёта о выполненной работе	339
Контрольные вопросы	339
4.6. Лабораторная работа № 6. Настройка сетевого взаимодействия	340
Цель работы	340
Краткие теоретические сведения	340
Используемое методическое и лабораторное обеспечение	343
Порядок выполнения работы	344
Содержание отчёта о выполненной работе	350
Контрольные вопросы	350
4.7. Лабораторная работа № 7. Конфигурирование службы Astra Linux Directory	351
Цель работы	351
Краткие теоретические сведения	351
Используемое методическое и лабораторное обеспечение	354
Порядок выполнения работы	354
Содержание отчёта о выполненной работе	363
Контрольные вопросы	363
4.8. Лабораторная работа № 8. Управление программными пакетами. Настройка системных служб	363
Цель работы	363
Краткие теоретические сведения	364
Используемое методическое и лабораторное обеспечение	367
Порядок выполнения работы	367

Содержание отчёта о выполненной работе	375
Контрольные вопросы	376
4.9. Лабораторная работа № 9. Настройка защищенного режима работы ОССН в соответствии с Astra Linux Red-Book	376
Цель работы	376
Краткие теоретические сведения	376
Используемое методическое и лабораторное обеспечение	377
Порядок выполнения работы	377
Содержание отчёта о выполненной работе	387
Контрольные вопросы	388
Список используемых сокращений	389
Литература	390