

П. Н. Девянин, В. Ю. Тележников, С. В. Третьяков

**Основы
безопасности
операционной
системы
Astra Linux
Special Edition**

УПРАВЛЕНИЕ ДОСТУПОМ



Оглавление

Предисловие.....	3
1. Базовый уровень защищенности («Орёл»).....	8
1.1. Дискреционное управление доступом.....	8
1.1.1. Учетные записи пользователей и групп.....	8
1.1.2. Аутентификация пользователей с использованием механизма РАМ.....	12
1.1.3. Файлы, каталоги и дискреционные права доступа к ним.....	15
1.2. Механизм расширения дискреционного управления доступом «Киоск-2».....	23
1.3. Особенности моделирования дискреционного (ролевого) управления доступом.....	27
1.3.1. Описание состояний системы.....	27
1.3.2. Описание правил перехода из состояний в состояния.....	33
1.3.3. Доказательство выполнения условий безопасности... Контрольные вопросы.....	37 39
2. Усиленный уровень защищенности («Воронеж»).....	41
2.1. Мандатный контроль целостности.....	41
2.1.1. Общий подход к реализации мандатного контроля целостности.....	41
2.1.2. Администрирование параметров мандатного контроля целостности.....	46
2.2. Статический контроль целостности (неизменности) файлов и замкнутая программная среда.....	53
2.3. Особенности моделирования мандатного контроля целостности.....	60
2.3.1. Описание состояний системы.....	60
2.3.2. Описание правил перехода из состояний в состояния.....	64
2.3.3. Доказательство выполнения условий безопасности... Контрольные вопросы.....	67 70
3. Максимальный уровень защищенности («Смоленск»).....	72
3.1. Общий подход к реализации мандатного управления доступом.....	72

3.2. Администрирование параметров мандатного управления доступом учётных записей пользователей и процессов	79
3.3. Администрирование параметров мандатного управления доступом файлов и каталогов	83
3.4. Особенности моделирования мандатного управления доступом	90
3.4.1. Описание состояний системы	90
3.4.2. Описание правил перехода из состояний в состояния	93
3.4.3. Доказательство выполнения условий безопасности... ..	98
Контрольные вопросы	102
4. Лабораторный практикум	104
4.1. Лабораторная работа № 1. Управление учетными записями пользователей и групп	104
Цель работы	104
Сведения, необходимые для выполнения работы	104
Порядок выполнения работы	107
4.2. Лабораторная работа № 2. Организация совместной работы с файлами и каталогами с помощью общей группы	109
Цель работы	109
Сведения, необходимые для выполнения работы	109
Порядок выполнения работы	112
4.3. Лабораторная работа № 3. Организация совместной работы с файлами и каталогами с помощью списков управления доступом	113
Цель работы	113
Сведения, необходимые для выполнения работы	113
Порядок выполнения работы	114
4.4. Лабораторная работа № 4. Использование дополнительных атрибутов файловой системы и привилегий для ограничения производимых с файлами операций	115
Цель работы	115
Сведения, необходимые для выполнения работы	116
Порядок выполнения работы	117
4.5. Лабораторная работа № 5. Использование механизмов «Киоск-2» и «Графический киоск» для расширения возможностей администрирования дискреционного управления доступом	119

Цель работы	119
Сведения, необходимые для выполнения работы	119
Порядок выполнения работы	120
4.6. Лабораторная работа № 6. Использование мандатного контроля целостности для администрирования ОССН	124
Цель работы	124
Сведения, необходимые для выполнения работы	124
Порядок выполнения работы	126
4.7. Лабораторная работа № 7. Организация файловой системы в рамках мандатного контроля целостности ..	127
Цель работы	127
Сведения, необходимые для выполнения работы	127
Порядок выполнения работы	128
4.8. Лабораторная работа № 8. Использование мандатного и дискреционного управления доступом для организации совместной работы с файлами и каталогами ..	129
Цель работы	129
Сведения, необходимые для выполнения работы	129
Порядок выполнения работы	131
4.9. Лабораторная работа № 9. Использование PARSEC-привилегий для восстановления данных из архивов .	134
Цель работы	134
Сведения, необходимые для выполнения работы	134
Порядок выполнения работы	135
4.10. Лабораторная работа № 10. Настройка ОССН для безопасной работы в соответствии с Astra Linux Red Book	135
Цель работы	135
Сведения, необходимые для выполнения работы	136
Порядок выполнения работы	138
Список используемых сокращений	141
Литература	142