

# Оглавление

---

<b>Предисловие</b> .....	17
<b>Благодарности</b> .....	18
<b>Об этой книге</b> .....	19
Кому следует прочитать эту книгу .....	20
Структура издания: дорожная карта .....	20
О коде .....	22
Дистрибутивы Linux .....	22
Форум книги .....	22
Другие интернет-ресурсы .....	23
От издательства .....	23
<b>Об авторе</b> .....	24
<b>Об иллюстрации на обложке</b> .....	25
<b>Глава 1.</b> Добро пожаловать в Linux .....	26
1.1. Что отличает Linux от других операционных систем .....	27
1.2. Основные сведения .....	28
1.2.1. Файловая система Linux .....	29
1.2.2. Начало работы: инструменты навигации в Linux .....	31
1.2.3. Начало работы: инструменты управления файлами Linux .....	36
1.2.4. Управление с клавиатуры .....	40
1.2.5. Псевдофайловые системы.....	41
1.2.6. Покажите, кто в доме хозяин: sudo.....	42

1.3.	Получение справки .....	43
1.3.1.	Map-файлы .....	43
1.3.2.	Команда info .....	44
1.3.3.	Всемирная паутина .....	45
Резюме .....		47
	Ключевые понятия .....	47
	Рекомендации по безопасности .....	47
	Обзор команд .....	47
	Самотестирование .....	48
<b>Глава 2.</b>	<b>Виртуализация Linux: создание безопасной и простой рабочей среды .....</b>	<b>50</b>
2.1.	Что такое виртуализация .....	51
2.2.	Работа с VirtualBox .....	55
2.2.1.	Работа с менеджерами пакетов Linux .....	56
2.2.2.	Определение виртуальной машины (VM) .....	63
2.2.3.	Установка операционной системы .....	67
2.2.4.	Клонирование и совместное использование виртуальной машины VirtualBox .....	71
2.3.	Работа с контейнерами Linux (LXC) .....	73
2.3.1.	Начало работы с LXC .....	73
2.3.2.	Создание вашего первого контейнера .....	74
Резюме .....		78
	Ключевые понятия .....	78
	Рекомендации по безопасности .....	79
	Обзор команд .....	79
	Самотестирование .....	80
<b>Глава 3.</b>	<b>Удаленное подключение: безопасный доступ к машинам по сети .....</b>	<b>82</b>
3.1.	Важность шифрования .....	82
3.2.	Начало работы с OpenSSH .....	84
3.3.	Вход на удаленный сервер по SSH .....	86
3.4.	Беспарольный доступ по SSH .....	88
3.4.1.	Генерация новой пары ключей .....	89
3.4.2.	Копирование открытого ключа по сети .....	91
3.4.3.	Работа с несколькими ключами шифрования .....	92
3.5.	Безопасное копирование файлов с помощью SCP .....	93
3.6.	Использование удаленных графических программ через соединения SSH .....	94
3.7.	Управление процессами в Linux .....	95
3.7.1.	Просмотр процессов с помощью команды ps .....	96
3.7.2.	Работа с systemd .....	98

Резюме .....	99
Ключевые понятия .....	100
Рекомендации по безопасности .....	100
Обзор команд .....	100
Самотестирование .....	101

**Глава 4.** Управление архивами: создание резервных копий или копирование  
целых файловых систем .....

4.1. Зачем архивировать .....	104
4.1.1. Сжатие .....	105
4.1.2. Архивы: некоторые важные соображения .....	105
4.2. Что архивировать .....	107
4.3. Где создавать резервную копию .....	109
4.4. Архивирование файлов и файловых систем с помощью инструмента tar .....	110
4.4.1. Примеры простого архива и сжатия .....	110
4.4.2. Поточковая архивация файловой системы .....	112
4.4.3. Сбор файлов с помощью инструмента find .....	114
4.4.4. Сохранение разрешений и прав собственности... и извлечение архивов .....	115
4.5. Архивирование разделов с помощью инструмента dd .....	119
4.5.1. Работа с инструментом dd .....	120
4.5.2. Стирание дисков с помощью инструмента dd .....	121
4.6. Синхронизация архивов с помощью инструмента rsync .....	121
4.7. Вопросы планирования .....	123
Резюме .....	125
Ключевые понятия .....	125
Рекомендации по безопасности .....	125
Обзор команд .....	126
Самотестирование .....	126

**Глава 5.** Автоматизированное администрирование: настройка автоматического  
резервного копирования .....

5.1. Сценарии с Bash .....	129
5.1.1. Пример сценария резервного копирования системных файлов .....	129
5.1.2. Пример сценария для изменения имен файлов .....	134
5.2. Резервное копирование данных в системе AWS S3 .....	136
5.2.1. Установка интерфейса командной строки AWS (CLI) .....	136
5.2.2. Настройка аккаунта AWS .....	137
5.2.3. Создание корзины AWS .....	139
5.3. Планирование регулярного резервного копирования с помощью инструмента cron .....	140

---

## 10 Оглавление

5.4.	Планирование нерегулярного резервного копирования с помощью инструмента anasron .....	142
5.4.1.	Запуск задания синхронизации S3 .....	143
5.5.	Планирование регулярного резервного копирования с помощью таймеров systemd .....	144
Резюме .....		146
Ключевые понятия .....		147
Рекомендации по безопасности .....		147
Обзор команд .....		147
Самотестирование .....		148
<b>Глава 6.</b>	<b>Инструменты для критических ситуаций: создание устройства для восстановления системы .....</b>	<b>150</b>
6.1.	Работа в режиме восстановления .....	152
6.1.1.	Системный загрузчик GRUB .....	153
6.1.2.	Использование режима восстановления в Ubuntu .....	154
6.1.3.	Использование режима восстановления в CentOS .....	155
6.1.4.	Поиск средств восстановления из командной строки .....	155
6.2.	Создание загрузочного диска восстановления .....	157
6.2.1.	Образы аварийного восстановления системы .....	157
6.2.2.	Запись образов на загрузочные USB-накопители .....	159
6.3.	Запуск загрузочного диска для работы .....	162
6.3.1.	Тестирование системной памяти .....	162
6.3.2.	Поврежденные разделы .....	165
6.3.3.	Восстановление файлов из поврежденной файловой системы .....	168
6.4.	Восстановление пароля: монтирование файловой системы с помощью инструмента chroot .....	170
Резюме .....		171
Ключевые понятия .....		171
Рекомендации по безопасности .....		172
Обзор команд .....		172
Самотестирование .....		172
<b>Глава 7.</b>	<b>Веб-серверы: создание сервера MediaWiki .....</b>	<b>174</b>
7.1.	Создание сервера LAMP .....	175
7.2.	Настройка веб-сервера Apache вручную .....	177
7.2.1.	Установка веб-сервера Apache на Ubuntu .....	177
7.2.2.	Заполнение корневого каталога документов сайта .....	178
7.3.	Установка базы данных SQL .....	179
7.3.1.	Усиление защиты SQL .....	181
7.3.2.	Администрирование SQL .....	182

7.4.	Установка PHP.....	185
7.4.1.	Установка PHP в Ubuntu.....	185
7.4.2.	Тестирование установки PHP.....	185
7.5.	Установка и настройка MediaWiki.....	186
7.5.1.	Диагностика недостающих расширений.....	188
7.5.2.	Подключение MediaWiki к базе данных.....	190
7.6.	Установка веб-сервера Apache на CentOS.....	192
7.6.1.	Общие сведения о сетевых портах.....	193
7.6.2.	Управление сетевым трафиком.....	194
7.6.3.	Установка MariaDB на CentOS.....	195
7.6.4.	Установка PHP на CentOS.....	195
Резюме.....		197
Ключевые понятия.....		198
Рекомендации по безопасности.....		198
Обзор команд.....		198
Самотестирование.....		199
<b>Глава 8.</b>	<b>Совместное использование файлов в сети: создание сервера для совместного использования файлов Nextcloud.....</b>	<b>201</b>
8.1.	Корпоративный файлообменник и Nextcloud.....	202
8.2.	Установка Nextcloud с помощью моментальных снимков.....	203
8.3.	Установка Nextcloud вручную.....	206
8.3.1.	Предварительные требования к оборудованию.....	206
8.3.2.	Построение сервера LAMP.....	207
8.3.3.	Конфигурирование Apache.....	208
8.3.4.	Скачивание и распаковка Nextcloud.....	210
8.4.	Администрирование Nextcloud.....	213
8.5.	Использование AWS S3 в качестве основного хранилища Nextcloud.....	216
Резюме.....		219
Ключевые термины.....		219
Рекомендации по безопасности.....		219
Обзор команд.....		220
Самотестирование.....		220
<b>Глава 9.</b>	<b>Защита вашего веб-сервера.....</b>	<b>222</b>
9.1.	Очевидные вещи.....	223
9.2.	Контролирование доступа к сети.....	225
9.2.1.	Настройка брандмауэра.....	225
9.2.2.	Использование нестандартных портов.....	232

9.3.	Шифрование данных при передаче.....	234
9.3.1.	Подготовка домена вашего сайта.....	236
9.3.2.	Генерация сертификатов с использованием Let's Encrypt.....	237
9.4.	Усиление процесса аутентификации.....	238
9.4.1.	Контроль за объектами файловой системы с помощью SELinux.....	239
9.4.2.	Установка и активация SELinux.....	241
9.4.3.	Применение политик SELinux.....	243
9.4.4.	Системные группы и принцип наименьших привилегий.....	244
9.4.5.	Изоляция процессов в контейнерах.....	247
9.4.6.	Сканирование на наличие опасных идентификаторов пользователей.....	247
9.5.	Аудит системных ресурсов.....	248
9.5.1.	Сканирование на наличие открытых портов.....	248
9.5.2.	Сканирование на предмет активных служб.....	249
9.5.3.	Поиск установленного программного обеспечения.....	250
Резюме.....		250
Ключевые термины.....		251
Обзор команд.....		251
Самотестирование.....		252
<b>Глава 10.</b>	<b>Защита сетевых соединений: создание VPN или DMZ.....</b>	<b>254</b>
10.1.	Создание туннеля OpenVPN.....	255
10.1.1.	Конфигурирование сервера OpenVPN.....	256
10.1.2.	Конфигурирование клиента OpenVPN.....	263
10.1.3.	Тестирование вашего VPN.....	265
10.2.	Построение сетей, защищенных от вторжений.....	267
10.2.1.	Демилитаризованные зоны (DMZ).....	267
10.2.2.	Использование iptables.....	270
10.2.3.	Создание DMZ с помощью iptables.....	271
10.2.4.	Создание DMZ с помощью Shorewall.....	273
10.3.	Построение виртуальной сети для тестирования инфраструктуры.....	276
Резюме.....		279
Ключевые термины.....		279
Обзор команд.....		280
Самотестирование.....		280
<b>Глава 11.</b>	<b>Мониторинг системы: работа с файлами журналов.....</b>	<b>282</b>
11.1.	Работа с системными журналами.....	283
11.1.1.	Журналирование с помощью journald.....	285
11.1.2.	Журналирование с помощью syslogd.....	287

11.2. Управление файлами журналов.....	289
11.2.1. Способ journald .....	289
11.2.2. Способ syslogd .....	289
11.3. Обработка больших файлов .....	291
11.3.1. Использование grep .....	291
11.3.2. Использование awk.....	292
11.3.3. Использование sed .....	293
11.4. Мониторинг с обнаружением вторжений .....	295
11.4.1. Настройка почтового сервера .....	296
11.4.2. Установка Tripwire.....	296
11.4.3. Конфигурирование Tripwire.....	299
11.4.4. Генерация тестового отчета Tripwire .....	301
Резюме .....	302
Ключевые понятия .....	302
Рекомендации по безопасности .....	303
Обзор команд.....	303
Самотестирование.....	304
<b>Глава 12. Совместное использование данных в частной сети.....</b>	<b>306</b>
12.1. Обмен файлами с помощью протокола сетевого доступа к файловым системам (NFS) .....	307
12.1.1. Настройка NFS-сервера.....	308
12.1.2. Настройка клиента.....	310
12.1.3. Монтирование общего ресурса NFS во время загрузки.....	311
12.1.4. Безопасность NFS .....	313
12.2. Обмен файлами с пользователями Windows с помощью Samba .....	315
12.2.1. Тестирование вашей конфигурации Samba .....	317
12.2.2. Доступ к серверу Samba из Windows.....	318
12.3. Совместное использование файлов с помощью символических ссылок.....	319
Резюме .....	321
Ключевые термины .....	321
Рекомендации по безопасности .....	321
Обзор команд.....	321
Самотестирование.....	322
<b>Глава 13. Устранение проблем производительности системы.....</b>	<b>324</b>
13.1. Проблемы с загрузкой процессора .....	325
13.1.1. Измерение загрузки процессора .....	325
13.1.2. Управление загрузкой процессора .....	326
13.1.3. Создание проблем (симуляция загрузки процессора).....	330

---

## 14 Оглавление

13.2.	Проблемы с памятью.....	330
13.2.1.	Оценка состояния памяти.....	330
13.2.2.	Оценка состояния свопа.....	331
13.3.	Проблемы доступности запоминающего устройства.....	332
13.3.1.	Ограничения inode.....	333
13.3.2.	Решение.....	335
13.4.	Проблемы с перегрузкой сети.....	335
13.4.1.	Измерение полосы пропускания.....	336
13.4.2.	Решения.....	337
13.4.3.	Формирование сетевого трафика с помощью команды tc.....	338
13.5.	Инструменты мониторинга.....	339
13.5.1.	Агрегирование данных мониторинга.....	339
13.5.2.	Визуализация ваших данных.....	341
Резюме.....		342
Ключевые термины.....		343
Рекомендации по безопасности.....		343
Обзор команд.....		343
Самотестирование.....		344
<b>Глава 14.</b>	<b>Устранение неполадок в сети.....</b>	<b>346</b>
14.1.	Понимание адресации TCP/IP.....	347
14.1.1.	Что такое адресация NAT.....	348
14.1.2.	Работа с адресацией NAT.....	348
14.2.	Установление сетевого подключения.....	351
14.3.	Устранение неполадок исходящего соединения.....	352
14.3.1.	Отслеживание статуса вашей сети.....	353
14.3.2.	Назначение IP-адресов.....	354
14.3.3.	Конфигурирование службы DNS.....	358
14.3.4.	Обслуживание сети.....	360
14.4.	Устранение неполадок при входящем соединении.....	361
14.4.1.	Сканирование внутреннего соединения: netstat.....	361
14.4.2.	Сканирование внешнего соединения: netcat.....	362
Резюме.....		363
Ключевые понятия.....		364
Рекомендации по безопасности.....		364
Обзор команд.....		364
Самотестирование.....		365



<b>Глава 15.</b> Устранение неполадок с периферийными устройствами .....	367
15.1. Идентификация подключенных устройств .....	368
15.2. Управление периферийными устройствами с помощью модулей ядра Linux .....	370
15.2.1. Поиск модулей ядра.....	371
15.2.2. Загрузка модулей ядра вручную .....	373
15.3. Ручное управление параметрами ядра во время загрузки .....	374
15.3.1. Передача параметров во время загрузки .....	374
15.3.2. Передача параметров через файловую систему.....	376
15.4. Управление принтерами.....	376
15.4.1. Основы lp .....	377
15.4.2. Управление принтерами с помощью CUPS.....	377
Резюме .....	379
Ключевые понятия .....	380
Рекомендации по безопасности .....	380
Обзор команд.....	380
Самотестирование.....	380
<b>Глава 16.</b> Инструменты DevOps: развертывание серверной среды с использованием Ansible.....	382
16.1. Чем полезна оркестровка развертывания .....	384
16.2. Ansible: установка и настройка .....	386
16.2.1. Настройка беспарольного доступа к хостам .....	386
16.2.2. Организация Ansible-хостов .....	387
16.2.3. Тестирование подключения .....	388
16.3. Аутентификация.....	389
16.4. Сценарии Ansible playbook.....	391
16.4.1. Написание простого playbook.....	391
16.4.2. Создание многоуровневых ролевых сценариев playbook .....	393
16.4.3. Управление паролями в Ansible.....	396
Резюме .....	397
Ключевые понятия .....	397
Рекомендации по безопасности .....	397
Обзор команд.....	398
Самотестирование.....	398
<b>Заключение</b> .....	400
Что вы узнали.....	400
Виртуализация.....	400

Связь .....	401
Шифрование.....	401
Сетевое взаимодействие.....	401
Управление образами .....	401
Системный мониторинг .....	402
Что дальше.....	402
Ресурсы .....	403
<b>Приложение. Обзор команд по главам.....</b>	<b>404</b>
Глава 1. Добро пожаловать в Linux.....	404
Глава 2. Виртуализация Linux: создание безопасной и простой рабочей среды.....	404
Глава 3. Удаленное подключение: безопасный доступ к машинам по сети.....	405
Глава 4. Управление архивами: создание резервных копий или копирование целых файловых систем .....	405
Глава 5. Автоматизированное администрирование: настройка автоматического резервного копирования.....	406
Глава 6. Инструменты для критических ситуаций: создание устройства для восстановления системы .....	406
Глава 7. Веб-серверы: создание сервера MediaWiki .....	407
Глава 8. Совместное использование файлов в сети: создание сервера для совместного использования файлов Nextcloud.....	407
Глава 9. Защита вашего веб-сервера .....	408
Глава 10. Защита сетевых соединений: создание VPN или DMZ .....	408
Глава 11. Мониторинг системы: работа с файлами журналов .....	409
Глава 12. Совместное использование данных в частной сети.....	409
Глава 13. Устранение проблем производительности системы .....	410
Глава 14. Устранение неполадок в сети .....	410
Глава 15. Устранение неполадок с периферийными устройствами .....	411
Глава 16. Инструменты DevOps: развертывание серверной среды с использованием Ansible.....	411