УДК 004.451
ББК 32.973.26-018.2
Ф71

Фленов М. Е.

Ф71 Linux глазами хакера. — 5-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2019. — 416 с.: ил.

ISBN 978-5-9775-4039-1

Рассмотрены вопросы настройки ОС Linux на максимальную производительность и безопасность. Описано базовое администрирование и управление доступом, настройка Firewall, файлообменный сервер, WEB-, FTP- и Proxy-сервера, программы для доставки электронной почты, службы DNS, а также политика мониторинга системы и архивирование данных. Приведены потенциальные уязвимости, даны рекомендации по предотвращению возможных атак и показано, как действовать при атаке или взломе системы, чтобы максимально быстро восстановить ее работоспособность и предотвратить потерю данных. В пятом издании информация представлена на примерах двух популярных дистрибутивов: CentOS и Ubuntu. На сайте издательства размещены дополнительная документация и программы в исходных кодах.

Для пользователей, администраторов и специалистов по безопасности

УДК 004.451
ББК 32.973.26-018.2

Группа подготовки издания:

Руководитель проекта	*Евгений Рыбаков*
Зав. редакцией	*Екатерина Сависте*
Компьютерная верстка	*Ольги Сергиенко*
Дизайн серии	*Марины Дамбиевой*
Оформление обложки	*Елизаветы Романовой*

"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

ISBN 978-5-9775-4039-1

Оглавление

Предисловие **11**
QualitySource 16
Второе издание 18
Третье издание 18
Четвертое издание 18
Пятое издание 19
Благодарности 20

Глава 1. Прежде чем начать **23**
1.1. Ядро 24
1.2. Дистрибутивы 25
1.2.1. Red Hat Linux 26
1.2.2. Slackware 26
1.2.3. SuSE Linux 27
1.2.4. Debian 27
1.2.5. Ubuntu 27
1.2.6. Raspbian 28

Глава 2. Установка и начальная настройка Linux **29**
2.1. Подготовка к установке 29
2.2. Начало установки 31
2.3. Разбивка диска 32
2.3.1. Файловые системы 34
2.3.2. Ручное создание разделов 36
2.4. Выбор пакетов для установки 39
2.5. Завершение установки 42
2.6. Пароль 43
2.7. Первый старт 46
2.8. Мы в системе 50
2.9. Подсказки 52
2.10. Основы конфигурирования 52
2.10.1. Запрещено то, что не разрешено 52
2.10.2. Настройки по умолчанию 53
2.10.3. Пароли по умолчанию 53

2.10.4. Безопасность против производительности....54
2.10.5. Внимательность....55
2.11. Обновление....56
2.12. Устройство Linux: ядро и модули....56
2.13. Установка дополнительных пакетов в Ubuntu....57
2.14. Установка дополнительных пакетов в CentOS....59
2.15. Редактирование файлов....60

Глава 3. Добро пожаловать в Linux....63
3.1. Файловая система....64
3.1.1. Основные команды....66
pwd....66
ls....66
cat....67
tac....68
cd....68
cp....68
find....69
grep....71
mkdir....71
rm....72
df....72
mount....72
umount....75
tar....76
rpm....76
which....76
3.1.2. Безопасность файлов....77
Дата изменения....77
Контрольные суммы....78
Что контролировать?....79
Замечания по работе с файлами....80
3.1.3. Ссылки....81
Жесткие ссылки....81
Символьные ссылки....82
3.2. Загрузка системы....84
3.2.1. Автозагрузка....84
3.2.2. GRUB2....86
3.2.3. Интересные настройки загрузки....87
3.3. Регистрация в системе....88
3.3.1. Теневые пароли....89
3.3.2. Забытый пароль....90
3.3.3. Модули аутентификации....91
3.3.4. Сложность паролей....92
3.4. Процессы....93
3.4.1. Смена режима....94
3.4.2. Остановка процессов....95
3.4.3. Просмотр процессов....96
3.4.4. «Зомби»: поиск и устранение....98

3.5. Планирование задач 100
3.5.1. Формирование задания 100
3.5.2. Планировщик задач 101
3.5.3. Безопасность запланированных работ 103
3.6. Настройка сети 104
3.6.1. Адресация 105
3.6.2. Информация о сетевых подключениях 106
3.6.3. Изменение параметров сетевого подключения 107
3.6.4. Утилита ip 108
3.6.5. Базовые настройки сети 109
3.6.6. Протокол IPv6 110
3.7. Работа с модулями ядра 111
3.8. Переменная *$PATH* 113

Глава 4. Управление доступом 115
4.1. Права доступа 115
4.1.1. Назначение прав 117
4.1.2. Владелец файла 119
4.1.3. Правила безопасности 119
4.1.4. Права по умолчанию 120
4.1.5. Права доступа к ссылкам 121
4.1.6. Права доступа к ссылкам 122
4.2. Управление группами 124
4.2.1. Добавление группы 124
4.2.2. Редактирование группы 125
4.2.3. Удаление групп 126
4.3. Управление пользователями 126
4.3.1. Файлы и папки нового пользователя 129
4.3.2. Изменение настроек по умолчанию 130
4.3.3. Редактирование пользователя 131
4.3.4. Удаление пользователя 131
4.3.5. Настройка процедуры добавления пользователей 132
4.3.6. Взлом паролей 134
4.4. Типичные ошибки распределения прав 135
4.5. Привилегированные программы 137
4.6. Дополнительные возможности защиты 137
4.7. Защита служб 139
4.7.1. Принцип работы 141
4.7.2. Установка Jail 142
4.7.3. Работа с программой Jail 143
4.8. Получение прав root 145
4.9. Права приложений 146
4.10. Сетевой экран 147
4.10.1. Фильтрация пакетов 149
4.10.2. Параметры фильтрации 150
Протоколы 152
Фильтрация портов 152
Фильтрация адресов 153
Фильтрация нежелательных адресов 154

Фильтрация неверных адресов 154
Фильтрация в Linux 155
4.10.3. Брандмауэр — не панацея 156
4.10.4. Брандмауэр как панацея 156
4.10.5. Конфигурирование брандмауэра 157
4.10.6. Основные возможности *iptables* 158
4.10.7. Переадресация 161
4.10.8. Утилита firewalld 162
4.10.9. Uncomplicated Firewall: упрощенное управление 162
4.11. Некоторые нюансы работы с брандмауэром 163
4.11.1. Обход сетевого экрана 164
4.11.2. Безопасный Интернет 166
4.11.3. Дополнительная защита 167
4.12. Запрет и разрешение хостов 168
4.13. Советы по конфигурированию брандмауэра 170
4.14. Повышение привилегий 171

Глава 5. Администрирование 177
5.1. Полезные команды для сетевых соединений 177
5.1.1. *ping* 178
5.1.2. *netstat* 179
5.1.3. *telnet* 180
5.1.4. *r*-команды 182
5.2. Шифрование 182
5.2.1. Программа stunnel 188
5.2.2. Дополнительные возможности OpenSSL 189
5.2.3. Шифрование файлов 191
5.2.4. Туннель глазами хакера 192
5.3. Протокол SSH 194
5.3.1. Конфигурационные файлы 194
5.3.2. Основные параметры конфигурации сервера SSH 195
5.3.3. Параметры доступа к серверу *sshd* 198
5.3.4. Конфигурирование клиента SSH 198
5.3.5. Пример работы клиента SSH 200
5.3.6. Вход по ключу 200
5.3.7. Защищенная передача данных 202
5.4. Демон *inetd/xinetd* 203
5.4.1. Конфигурирование *xinetd* 204
5.4.2. Безопасность 206

Глава 6. В стиле Samba 209
6.1. Конфигурирование Samba 210
6.1.1. Основные настройки 212
6.1.2. Безопасность 213
6.1.3. Сеть 215
6.1.4. Замена сервера Windows 215
6.1.5. Поддержка WINS и DNS 216
6.1.6. Отображение файлов 216

6.2. Описание объектов 217
6.2.1. Пора домой 217
6.2.2. Доменный вход 218
6.2.3. Распечатка 218
6.2.4. Общий доступ 219
6.2.5. Личные каталоги 219
6.2.6. CD-ROM 220
6.3. Управление пользователями 221
6.4. Использование Samba 222
6.5. Развитие Samba 224

Глава 7. Веб-сервер 225
7.1. Основные настройки 226
7.2. Модули 228
7.3. Права доступа 229
7.4. Создание виртуальных веб-серверов 235
7.5. Еще несколько слов о безопасности 236
7.5.1. Файлы *.htaccess* 237
7.5.2. Файлы паролей 238
7.5.3. Проблемы авторизации 240
7.5.4. Обработка на сервере 240
7.6. Проще, удобнее, быстрее 241
7.7. Безопасность сценариев 242
7.7.1. Основы безопасности сценариев 243
7.7.2. Модуль mod_security 245
7.7.3. Секреты и советы 246
Ограничение сценариев 247
Резервные копии 247
7.8. Индексация веб-страниц 248
7.9. Безопасность подключения 250

Глава 8. Электронная почта 253
8.1. Настройка sendmail 255
8.2. Работа почты 257
8.2.1. Настройка сервера для отправки почты 258
8.2.2. Настройка сервера для чтения почты 259
8.2.3. Безопасность сообщений 261
8.3. Полезные команды 261
8.4. Безопасность sendmail 262
8.4.1. Баннер-болтун 262
8.4.2. Только отправка почты 262
8.4.3. Права доступа 263
8.4.4. Лишние команды 263
8.4.5. Выполнение внешних команд 264
8.4.6. Доверенные пользователи 264
8.4.7. Отказ от обслуживания 264
8.5. Почтовая бомбардировка 265

8.6. Спам 266
8.6.1. Блокировка приема спама 266
Фильтрация серверов 266
Фильтрация сообщений 267
8.6.2. Блокировка пересылки спама 269
8.7. Сервер Postfix 270
8.7.1. Псевдонимы 271
8.7.2. Ретрансляция 272

Глава 9. Шлюз в Интернет 273
9.1. Работа прокси-сервера 273
9.2. Кэширование 278
9.3. Прокси-сервер squid 278
9.3.1. Директивы настройки HTTP 278
9.3.2. Директивы настройки FTP 279
9.3.3. Настройка кэша 280
9.3.4. Журналы 282
9.3.5. Разделение кэша 283
9.3.6. Дополнительные директивы 284
9.4. Права доступа к squid 285
9.4.1. Список контроля доступа 285
9.4.2. Определение прав 287
9.4.3. Аутентификация 287
9.5. Некоторые нюансы работы со squid 289
9.5.1. Безопасность сервиса 289
9.5.2. Ускорение сайта 289
9.5.3. Маленький секрет поля *User Agent* 289
9.5.4. Защита сети 290
9.5.5. Борьба с баннерами и всплывающими окнами 290
9.5.6. Подмена баннера 292
9.5.7. Борьба с запрещенными сайтами 295
9.5.8. Ограничение канала 295
9.6. Защита прокси-сервера: squidGuard 299
9.6.1. Установка 299
9.6.2. Настройка 300
9.7. Шлюз в Интернет 302

Глава 10. Передача файлов 305
10.1. Протокол FTP 306
10.1.1. Команды протокола FTP 306
10.1.2. Сообщения сервера 309
10.1.3. Передача файлов 311
10.1.4. Режим канала данных 312
10.2. Сервер ProFTPd 313
10.3. Еще несколько слов о протоколе FTP 315

Глава 11. DNS-сервер 317
11.1. Введение в DNS 318
11.2. Локальный файл hosts 319

11.3. Внешние DNS-серверы 320
11.4. Настройка DNS-сервиса 321
11.5. Файлы описания зон 323
11.6. Обратная зона 325
11.7. Безопасность DNS 326

Глава 12. Мониторинг системы 329
12.1. Автоматизированная проверка безопасности 330
12.2. Закрываем SUID- и SGID-двери 333
12.3. Проверка конфигурации 334
12.4. Журналирование 337
12.4.1. Основные команды 337
who 337
users 338
last 338
history 339
lastlog 339
lsof 340
12.4.2. Системные текстовые журналы 341
12.4.3. Журнал FTP-сервера 342
12.4.4. Журнал прокси-сервера squid 344
12.4.5. Журнал веб-сервера 345
12.4.6. Кто пишет? 345
12.4.7. Утилита logrotate 351
12.4.8. Пользовательские журналы 353
12.4.9. Обратите внимание! 354
12.5. Работа с журналами 356
12.5.1. Команда *tail* 357
12.5.2. Программа swatch 358
12.5.3. Программа Logsurfer 358
12.5.4. Программа Logcheck/LogSentry 358
12.6. Безопасность журналов 359
12.7. Мониторинг ресурсов 361

Глава 13. Резервное копирование и восстановление 363
13.1. Основы резервного копирования 363
13.2. Доступность на все 100 процентов 365
13.3. Хранение резервных копий 366
13.4. Политика резервирования 367
13.4.1. Редко, но метко 368
13.4.2. Зачастили... 368
13.4.3. Часто, но не все... 369
13.4.4. Периодично 369
13.4.5. Полная копия... 370
13.5. Резервирование в Linux 370
13.5.1. Копирование 370
13.5.2. Утилита tar 371
13.5.3. Утилита gzip 373
13.5.4. Утилита dump 374

13.6. Защита резервных копий....375
13.7. Облака....376

Глава 14. Советы на прощанье....377
14.1. Пароли....377
14.2. rootkit: «набор администратора»....380
14.3. backdoor: «потайные двери»....383
14.4. Небезопасный NFS....384
14.5. Определение взлома....386
14.5.1. Осведомлен — значит защищен....386
14.5.2. Ловля на живца....388
14.6. Тюнинг ОС Linux....390
14.6.1. Параметры ядра....390
14.6.2. Тюнинг HDD....393
14.6.3. Автомонтирование....395
14.7. Короткие советы....397
14.7.1. Дефрагментация пакетов....397
14.7.2. Маршрутизация от источника....397
14.7.3. SNMP....398
14.7.4. Полный путь....398
14.7.5. Доверенные хосты....399

Заключение....401

Приложение 1. Команды протокола FTP....403

Приложение 2. Полезные программы....405

Приложение 3. Интернет-ресурсы....407

Приложение 4. Работа в командной строке....409
Псевдонимы....409
Перенаправление....410
Запуск в фоне....410
Последовательность команд....411

Предметный указатель....412

Предисловие

Эта книга посвящена рассмотрению одной из самых популярных операционных систем (ОС), устанавливаемых на серверы, — ОС Linux. А если учесть, что Андроид тоже построен на базе Linux, то и этой мобильной ОС.

Для домашнего использования ОС Linux за долгие годы своего существования пока еще не получила такой популярности, как среди профессиональных администраторов. На мой взгляд, проблема кроется в графическом интерфейсе и отсутствии необходимых программ. Но это мое личное мнение.

Графические оболочки Linux выполнены в достаточно спорном дизайне. Рабочую среду GNOME и ее разработчиков раскритиковал даже сам создатель Linux — Линус Торвальдс.

Я больше предпочитаю классические, простые и строгие цвета и, наверное, поэтому последние два года больше всего времени провожу в macOS, которая является достаточно близким родственником Linux, потому что построена на компонентах BSD (обе ОС имеют UNIX-корни). Ядро, которое используется в macOS, когда-то создавалось программистами BSD, хотя его присутствие в ее дистрибутивах никогда официально не признавалось. Плюс очень много утилит в эту ОС от Apple также пришли из мира UNIX.

Операционная система macOS и различные дистрибутивы Linux очень схожи — много общего в работе консоли, а такие понятия, как конфигурация MySQL, PHP, Apache, вообще идентичны.

Второй недостаток Linux — нехватка хороших программ. Опять же, для Windows и macOS существуют MS Office и вся линейка продуктов Adobe, а бесплатные офисные пакеты под Linux пока все еще очень сильно проигрывают MS Office. Да и Adobe Photoshop до сих пор остается бесспорным лидером. Это снова мое личное мнение — кому-то The GIMP может быть удобен и Google Docs достаточно.

Но вот что касается серверных приложений, где не нужно никаких красот, а требуются лишь производительность и надежность, и достаточно просто командной строки или управления через удаленный терминал или браузер, — то тут все преимущества Linux выходят на первый план, и здесь она способна конкурировать

с другими ОС. Недаром большинство серверов строят именно на Linux, потому что ее серверные компоненты вполне конкурентоспособны с аналогами из других платформ и даже превосходят их.

Лично я использую Linux, главным образом, как серверную систему и, в основном, в Сети. Она бесплатная, и это позволяет сэкономить пользователям и компаниям во всем мире огромные суммы денег на лицензиях. По работе мне приходится иметь дело с серверами как на Windows, так и на Linux, и вторые обходятся намного дешевле, так что для своих проектов я всегда выбираю их.

Установка ОС Linux становится проще, а графический интерфейс и удобство работы в некоторых случаях не уступают самой распространенной на настольных системах операционной системе Windows. Самое главное, что ценят пользователи Linux, — это возможность ее настраивать.

Когда-то Windows 9*x* и даже Windows XP можно было настраивать на любой вкус, и существовали программы, которые изменяли внешний вид рабочего стола до неузнаваемости. В Windows Vista возможности по настройке сильно сократились, а с полным изменением рабочего стола в Windows 8/10 менять стало практически нечего.

За долгие годы существования Linux осталась гибкой. На нее можно устанавливать различные графические оболочки, можно даже сделать так, что рабочий стол станет выглядеть как Windows, как macOS или даже как нечто космическое. Именно за эту гибкость Linux любят во всем мире.

Почему же тогда гибкость настройки не помогает процветанию системы? Мое мнение — просто это мало кому нужно. Когда я был студентом, то сам любил настраивать ОС под себя, изменять ее вид, что-то менять в ее недрах. Сейчас, когда у меня есть работа, семья, дети — времени на подобные развлечения уже не остается. Мне нужно включить компьютер и начать работать с ним сразу, без каких-либо дополнительных настроек.

Для таких, как я, важно, чтобы ОС была удобна и красива уже «из коробки». А понятия удобства и красоты — это дело вкуса каждого. Так, мне нравились Windows до 8-й ее версии, и только 8-ю я так и не смог понять. Мне нравится macOS, но почему-то за долгие годы я так и не смог полюбить оболочку рабочего стола Unity, которая долго использовалась в Ubuntu.

Мы будем рассматривать в этой книге Ubuntu (ее корни — Debian) и немного затронем CentOS. Согласно статистике Интернета, Ubuntu является самой популярной сборкой Linux. Чтобы узнать эту статистику, достаточно зайти в рейтинг **mail.ru** и посмотреть любой популярный открытый сайт. Статистика **mail.ru** показывает, с каких ОС и с каких браузеров заходят на сайт пользователи. Так вот, среди дистрибутивов Linux с огромным отрывом на первом месте находится Ubuntu, поэтому имеет смысл выбрать именно ее.

CentOS сильно отличается от Ubuntu — у нее другой пакетный менеджер, и ее больше сравнивают с Red Hat Linux. Очень часто можно услышать, что CentOS — это бесплатная версия Red Hat. Не знаю, насколько верно это утверждение. Этот

дистрибутив я чаще вижу на веб-серверах, и мои сайты работают на выделенном хостинге именно под CentOS.

Я не смогу «покрыть» в этой книге обе ОС полностью и не планирую этого делать. Но я постараюсь вас ими заинтересовать и дать такую основу, чтобы дальше вы могли двигаться уже без меня.

В мире Linux — в различных ее дистрибутивах — используется значительное количество общих компонентов. Как я уже говорил ранее, macOS от компании Apple основана на BSD (одном из вариантов UNIX-систем), и в ней также очень много общего с Linux, — я могу без проблем копировать некоторые конфигурационные файлы с macOS на Linux, и они будут работать без изменений.

Почему так вызывающе называется книга? Это маркетинговый ход или просто какой-то трюк? Когда я написал первую книгу по программированию на Delphi, то основой для нее послужили статьи из журнала «Хакер». Тогда редакция и предложила мне название: «Delphi глазами хакера». Нет, это не мои глаза имелись тут в виду, имелся в виду стиль журнала, — ведь я тогда вплотную работал с ним и очень много для него писал. На обложке той книги даже слово «хакер» было набрано в стиле оформления журнала.

Впоследствии эти «глаза» стали использоваться и для других моих книг, хотя вид слова «хакер» на обложках пришлось изменить, — издательство «Gameland» запретило оформлять это слово их шрифтом.

В названии книги не имеется в виду, что хакер — в смысле взломщик — это я. Я как раз к таким никогда себя не относил, и больше предпочитаю создавать и защищать. Но в книге все же будут присутствовать глаза некоего взломщика, который будет смотреть на вашу систему извне. А чтобы понять, как защищаться, нужно понять, как думает тот, от кого вы защищаетесь, и знать, как он может атаковать.

Эта книга посвящена безопасности, но не только ей. В основном, мы будем говорить о самой Linux, и моя главная задача — погрузить вас в ее увлекательный и захватывающий мир. Я не стану пытаться описать всю систему, потому что для этого книга должна быть в несколько раз толще, — мы рассмотрим только самое интересное на мой взгляд.

Я интересуюсь взломом и постоянно изучаю новые его методы, но только потому, что хочу строить безопасные системы, и безопасность меня интересует намного больше. Любой объект может быть рассмотрен с разных точек зрения. Простой пример из жизни — нож, являясь столовым прибором, при определенных обстоятельствах становится орудием убийства или средством самообороны. Точно так же программные инструменты, утилиты или даже просто знания могут быть восприняты и как советы для повседневного ухода за ОС, и как способы защиты ее от проникновения, или же как средства взлома системы. Я надеюсь, что вы не станете использовать полученные знания в разрушительных целях. Это вас не украсит, и славы не добавит. Да и зачем вам нужна «черная» популярность взломщика? Не лучше ли посвятить себя более полезным и добрым вещам?

Причины, по которым люди идут темной дорогой, могут быть разными. Кто знает человека, который разработал средства безопасности для какой-либо крупной компании или сайта? Хотя бы одного из людей, отвечающих за безопасность крупных сайтов? Мало кто слышал о них... Но стоит взломать Facebook или любой другой сайт, как о вас заговорят во всем мире. Стремление к такой дешевой популярности понятно, но оно совершенно бессмысленно и не нужно.

Когда меня спрашивают, что я подразумеваю под словом «хакер», я привожу простейший пример — если вы как администратор установили и заставили работать ОС, и вам удалось настроить ее на максимальную производительность и безопасность, то вы — хакер. Умения хакера позволяют создавать что-либо, превосходящее имеющиеся аналоги (т. е. более быстрое, удобное и безопасное). Именно такой является сама ОС Linux, созданная хакерами со всего мира.

Для меня слово «хакер» ассоциируется с людьми, которые создают что-то, а не взламывают. И так считаю не только я. В Торонто уже не раз проходил Facebook Hack, на котором люди не взламывали самую популярную пока социальную сеть, а писали код, создавали приложения для Facebook и соревновались в умении программировать.

Наверное, пора более детально поговорить о том, что будет ожидать вас в самой книге.

Для того, чтобы установить ОС на домашний компьютер, не требуется много настроек. Большинство операционных систем устанавливаются с настройками по умолчанию вполне безопасно. Простому домашнему компьютеру не нужно открывать никаких сервисов внешнему миру. И только вы сами инициируете большинство соединений с внешним миром, запрашивая у почтовых серверов свою почту или у веб-серверов интересующие вас страницы, музыку и видео. Поэтому достаточно запретить любые входящие соединения и разрешить только то, что пользователь запросит сам. И если пользователь попросил систему соединить его с «не совсем хорошим» сервером, то это уже будет ошибка пользователя, потому что ОС и программы мало что могут в этом случае сделать.

Единственное, что нужно в качестве дополнительной защиты домашним компьютерам, — антивирусы, которые будут проверять контент, который пользователь получает/скачивает, на предмет возможного вредоносного кода. Пока что в Linux не было серьезных вирусных эпидемий, которые уже не раз захлестывали мир Windows, и большинство пользователей Linux не ставит антивирусов.

Можно поставить еще и сетевые экраны, которые будут защищать вас от возможных атак, но даже без них в современном мире можно прожить.

В случае с сервером все намного сложнее. Серверы для того и предназначены, чтобы предоставлять пользователям какой-то контент. К ним могут подключаться совершенно разные пользователи со всего мира, которых вы никогда не видели и не знали. Доверие к таким посетителям практически нулевое, потому что никогда не знаешь, кто запрашивает ресурсы сервера, для чего и как он собирается их использовать.

Мне кажется, что большинство недочетов в программах происходит как раз из-за недопонимания этого. Программисты просто не задумывались о потенциальных угрозах и надеялись, что пользователи будут делать только то, что для них предусмотрено. Но хакеры — далеко не ординарные пользователи, и они обязательно будут пытаться использовать то, что не должно быть доступно.

В результате настройка сервера превращается иногда в увлекательное приключение, где борются Инь и Янь: разрешить или запретить? Дать возможность или нет?

Для того чтобы правильно настроить сервер, необходимо знать множество параметров, которые большинству пользователей не нужны. Если же просто закрыть глаза и оставить все значения по умолчанию, то об истинной безопасности Linux не может быть и речи. Дело в том, что производитель программы заранее не знает, что именно нам понадобится, и делает все возможное, чтобы она работала на любой системе, а для этого ему приходится включать в нее много дополнительных возможностей, что делает систему в целом избыточной.

В последнее время разработчики дистрибутивов и других серверных программ стали максимально урезать установки по умолчанию, т. е. разрешать только базовые возможности, а все сетевые сервисы, которые могут позволить хакеру проникнуть на компьютер, отключать. При этом чаще всего производитель предоставляет нам простое и удобное средство для быстрого включения и конфигурирования нужного сервиса.

Так уж повелось, что администраторы Linux должны иметь больше опыта и знаний, чем специалисты Windows, и это связано как раз со сложностями настройки, осуществляемой с использованием конфигурационных файлов и утилит командной строки. Если в Windows все делается в визуальных окнах с большим количеством контекстных подсказок, то в Linux большинство настроек осуществляется именно в конфигурационных файлах. Да, для нее тоже существуют утилиты, упрощающие настройку, но функционал не всех их столь удобен и гибок, как простое прямое конфигурирование файлов.

Я всегда рекомендую, изучая какую-либо тему, узнать мнение еще как минимум двух-трех авторов. Так что обязательно возьмите еще несколько других книг. У каждого автора свой подход, и разные темы могут быть раскрыты по-разному. К тому же, в книгах часто можно встретить авторские описания собственного их опыта, а это самое важное и дорогое.

Можно, например, почитать работы Дениса Колисниченко, который уже не первый год специализируется в Linux. Я видел одну его книгу лет десять назад, и она мне показалась очень даже интересной. Хотелось прочитать ее полностью, но я уехал в Канаду, а отсюда у меня доступ к литературе на русском языке практически отсутствует. Онлайн-магазины не доставляют книги в Канаду, а качать нелегальные версии я не хочу. Впрочем, вроде бы сейчас издательства в России стали продавать электронные версии книг, и если это так, то я, наверное, смогу легально покупать книги на русском через Интернет.

Рассматривая Linux, я буду говорить о безопасности и производительности не в отдельных заключительных главах, а, практически, все время. Из-за этого могут

иногда случаться повторы, но я считаю, что это необходимо. Когда человек уже приобрел навыки неэффективной работы с системой, переучиваться ему сложно. Именно поэтому мы будем разбирать последовательно (от азов до сложных вопросов) все аспекты каждой рассматриваемой темы, аккуратно раскладывая полученные знания «по полочкам».

В качестве дополнительной информации по безопасности компьютера и сетей советую прочитать мою книгу «Компьютер глазами хакера»[1], в которой приводится достаточно много общих сведений по этим вопросам. Здесь же мы больший упор делаем на определенную ОС — Linux. Несмотря на то, что упомянутая книга направлена в большей степени на поддержание безопасности ОС Windows, многие рассматриваемые в ней проблемы могут вам пригодиться и при построении безопасного Linux-сервера. Точно так же книга «Linux глазами хакера» будет полезна и специалистам по безопасности Windows-систем.

В этой книге не рассматриваются вопросы, связанные с вирусами, потому что в настоящее время вирусная активность в ОС Linux минимальна, но это не значит, что опасности не существует вовсе. Угроза есть всегда, а защита от вирусов схожа с защитой от троянских программ, которых для Linux достаточно много. О вирусных атаках и возможностях их отражения можно также прочитать в книге «Компьютер глазами хакера».

Кстати, популярная сейчас на мобильных устройствах ОС Android построена на базе Linux, и появление под нее вредоносного кода показало, что и здесь вопросами безопасности пренебрегать не стоит.

Итак, давайте знакомиться с Linux с точки зрения хакера. Я уверен, что вы посмотрите на нее совершенно другими глазами и найдете для себя много нового и интересного.

QualitySource

Мой взгляд на Linux может вам понравиться, а может и шокировать. Дело в том, что я не принадлежу к сторонникам или поклонникам Open Source, к которому относится Linux. Я отношу себя к сторонникам движения QualitySource (такого реально не существует, это я так его для себя называю), т. е. качественного кода. Мне все равно, какой это код — открытый или закрытый, главное, чтобы он был качественный. Если бы код ОС Windows был открытым, вы бы полезли его смотреть или изменять? Я бы нет, и большинство тоже.

Я даже против изменения исходных кодов. Изменив их под себя один раз, вам придется делать это каждый раз, когда выходит новая версия. Само собой, что в вышедшем завтра обновлении ОС не окажется ваших изменений. Придется снова и снова изменять исходный код или создавать свою личную ветку кода и поддерживать ее самостоятельно. Но если каждый будет заниматься поддерживанием своих веток, то когда найти время на собственную жизнь и семью?

---

[1] См. **http://www.bhv.ru/books/book.php?id=189767**.

Когда только появился Android, то для него все производители начали писать свои оболочки, чтобы выделиться из общего фона. С выходом каждой новой версии этой ОС приходилось ждать, когда оболочки обновят. Это как топтание на месте — постоянно приходится адаптировать и тестировать один и тот же код для новой версии ОС. Всем это явно надоело, и все чаще можно видеть «чистую» ОС Андроид.

Большинство из нас, устанавливая ОС или какую-то программу, хочет, чтобы она стабильно работала и выполняла положенные действия. Какая нам разница, открыт код или нет? Какая нам разница, на каком языке написана программа? Для меня эти вопросы не существенны. Если программа стоит того, чтобы я отдал за нее запрашиваемые деньги, если она достаточно качественна, — то я отдам эти деньги, независимо от того, открыт ли ее код, и на каком языке ее написали.

И ОС Linux, и Windows, на мой взгляд, являются качественными проектами, и я использую их одновременно, но для разных задач. Устанавливать сложный, тяжеловесный и дорогой Windows Server ради банального файлового сервера — это глупость, поэтому здесь я использую Linux. Но для сложных финансовых решений я предпочитаю использовать великолепную связку MS Windows и MS SQL Server. Это мое личное предпочтение, которому не обязательно следовать. Вы можете выбрать для управления базой данных связку Linux и MySQL.

С 2009-го по 2017-й год я работал над сайтами с высокой нагрузкой и в качестве бэкэнда[1] использовал серверы Windows, на которых установлены база данных и веб-серверы (потому что для больших сайтов я все же предпочитаю использовать C#), но на фронтенде[2] у меня были установлены кэширующие серверы Linux, FTP-серверы на Linux, серверы деплоя (развертывания) и управления так же на Linux.

К какому миру присоединиться — это личное решение каждого. Единственное, о чем я прошу вас, — не делайте ничего бездумно. Не стоит устанавливать софт только потому, что он относится к Open Source, как и не стоит считать, что коммерческий софт заведомо лучше. Выбирайте своим умом, пробуйте, тестируйте и принимайте самостоятельное решение в зависимости от конкретной ситуации.

Программа не может быть лучше, надежнее или безопаснее других только потому, что у нее открыт код, это бред полнейший. Яркий пример — sendmail. Не очень хороших программ с открытым кодом, как, кстати, и коммерческих, весьма много, поэтому выбирайте за качество, а не за наличие или отсутствие исходных кодов, которые большинству пользователей просто не нужны.

Почему и когда я выбираю Linux? Я программист, который любит Microsoft .NET и PHP. Первый лучше выполнять на Windows-серверах, а второй на Linux. И если для финансовых проектов я выберу .NET за его возможности, то для любых других проектов я остановлюсь на Linux+Apache+MySQL+PHP (LAMP), как на более эко-

---

[1] Бэкэнд (от англ. Back-End, оборотная сторона) — программный код, отвечающий за работу с сервером (базой данных), данными (для их дальнейшей записи в БД или отправки клиенту) и т. п.

[2] Фронтенд (от англ. Front-End, лицевая сторона) — публичная часть сайта, с которой непосредственно контактирует пользователь, и функционал, который обычно обыгрывается на клиентской стороне (в браузере).

номном варианте. Эта связка не требует дорогих лицензий, отчисляемых Microsoft, а ее серверы будут потреблять меньше памяти.

Сейчас на сервере, где находятся мои сайты, мне выделено всего 512 мегабайт памяти, но монитор показывает, что используются около 300, и есть еще незанятое пространство. На виртуальную машину с таким количеством памяти поставить полноценную Windows не выйдет, — придется ставить только версию Core, для которой 512 Мбайт — минимум, и тут уже о комфортной работе говорить будет сложно. А если нужна Windows с возможностью удаленного подключения по RDP[1], то потребуется минимум 4 гигабайта, а это уже намного дороже.

Второе издание

Чем отличалось второе издание книги? Я бы назвал обе эти книги разными, потому что в новом варианте было приведено намного больше информации. Я переписал абсолютно все и обновил весь текст в соответствии с современными реалиями.

В ходе этой работы были исправлены и некоторые ошибки, присутствовавшие в предыдущем издании. Их было немного, но в Интернете по этому поводу очень красиво писали те, кто почему-то не любит меня и мои книги. Не знаю, почему — ведь я никому ничего плохого не сделал... Ошибки есть везде, даже в авторитетных американских изданиях. Просто там новые издания появляются каждый год, поэтому ошибки исправляются достаточно быстро.

Третье издание

В третьем издании я уже в основном обновлял информацию в соответствии с современными реалиями. Компьютерный мир изменяется очень быстро, за что я его и люблю, потому что приходится постоянно изучать что-то новое. Очень много новой информации попало на компакт-диск к этой книге в виде текстовых файлов.

Я хотел донести до читателя как можно больше информации, и при этом не делать книгу слишком толстой и дорогой. Единственный способ сделать это — максимально использовать компакт-диск. Наиболее интересная информация попала в книгу, чтобы ее было увлекательно читать. Некоторые сильно устаревшие участки текста ушли на компакт-диск.

Четвертое издание

Четвертое издание снова полностью переписано. Я опять пробежался по каждой главе и каждому абзацу и переделал очень многое. Компьютерный мир меняется сильно и быстро. Информация из первого издания уже совершенно не актуальна, и даже то, что я добавлял во втором издании, также сильно изменилось.

[1] RDP (Remote Desktop Protocol) — протокол удаленных рабочих столов.

В Linux поменялись приоритеты при выборе файлового или почтового сервера по умолчанию. Что остается до сих пор актуальным — так это связка LAMP (Linux, Apache, MySQL, PHP). Она, кажется, будет жить вечно, потому что эти четыре продукта на самом деле весьма качественные и отлично поддерживаются их создателями.

Я даже немного изменил подход к описанию программ и самой ОС. Если раньше я пытался описать как можно больше команд и параметров, то в этом издании я выкинул очень много скучных и лишних описаний и добавил то, что на мой взгляд будет более интересно читателям.

Даже если у вас есть любое из предыдущих изданий, это издание вам так же будет интересно прочесть практически полностью.

И еще одно изменение, произведенное для четвертого издания, — информация, расширяющая и дополняющая материал «бумажной» книги, теперь не приклеивается к ней в виде компакт-диска, а размещается на FTP-сервере издательства, и электронный архив с этой информацией можно скачать по ссылке **ftp://ftp.bhv.ru/9785977533331.zip** или со страницы 4-го издания книги на сайте **www.bhv.ru**.

Пятое издание

Пока еще рано переписывать всю книгу, потому что в предыдущем издании была проделана большая работа.

Тем не менее, в пятом издании я сократил количество вступительного материала и общих слов о Linux, его истории и пр. Все это переехало на мой сайт в раздел статей по адресу: **http://www.flenov.info/story/category/Linux**. Взамен я добавил больше практической информации о самой ОС Linux. Девиз этого издания: меньше общих слов — больше дела!

Обновлена информация по управлению сетевым экраном, добавлено немного новых примеров, включая Uncomplicated Firewall[1], описано, как настроить шлюз в Интернет. В главу о работе с почтой добавлен раздел по борьбе со спамом. Приведено больше информации по безопасности — этого много не бывает.

Все предыдущие издания описывали только Ubuntu, а в пятое я добавил информацию про CentOS, потому что это очень распространенный Linux-дистрибутив для серверов.

[1] Uncomplicated Firewall (ufw) — в переводе с англ. «незамысловатый межсетевой экран», обертка для брандмауэра iptables в Ubuntu.

Благодарности

В каждой своей книге я стараюсь поблагодарить всех, кто помогал в ее создании и выходе в свет. Без этих людей просто ничего бы не получилось.

Первым делом я хотел бы поблагодарить издательство «БХВ-Петербург», с которым сотрудничаю уже долгие годы. Спасибо руководству издательства, редакторам и корректорам, которые работают со мной и помогают сделать книгу такой, какой я ее задумывал. Ведь писать приходится в тяжелых по срокам условиях, но иначе нельзя — информация может устареть раньше, чем книга попадет на прилавок.

Спасибо всем, кто помогает сделать текст лучше, обложку красивой и книгу доступной всем желающим.

Не устану благодарить родителей, жену и детей за их терпение. После основной работы я прихожу домой и тружусь над очередной книгой. Таким образом, семья может видеть меня только за компьютером, а общаться со мной очень сложно, потому что все мои мысли устремляются далеко в виртуальную реальность.

Большая благодарность моим друзьям и знакомым, которые что-то подсказывали, помогали идеями и программами.

Так уж выходит, но в написании каждой книги участвуют и животные. Эта работа тоже не стала исключением. Во время подготовки первого издания книги мой кот Чекист с 23:00 до 1:00 ночи гулял по квартире и просто кричал от скуки. Я не мог уснуть, а значит, больше времени уделял работе.

Хочется поблагодарить еще одного кота — который служил ассистентом в пакете программ MS Office. Одно из первых изданий книги я писал в MS Word, а ОС Linux работала в виртуальной машине, чтобы можно было делать снимки экрана. Во время работы, если «на меня бросали» ребенка, вордовский кот-ассистент помогал занять моего годовалого сына, выступая в роли няни. Я сажал сына Кирилла рядом, и он спокойно играл с котом на экране монитора, а я мог продолжать работать над книгой. Правда, иногда приходилось спасать кота и монитор, когда сын пытался маленькой ручонкой неуклюже гладить полюбившееся животное.

Сейчас мой сын уже вырос, а это издание в основном писалось в автобусе по пути на работу и домой.

А самая большая благодарность: вам — за то, что купили книгу, и моим постоянным читателям, с которыми я регулярно общаюсь в моем блоге **www.flenov.info**. Последние мои работы основываются на их вопросах и предложениях. Если у вас появятся какие-либо проблемы, то милости прошу на сайт. Я постараюсь помочь по мере возможности, и жду любых комментариев по поводу этой книги. Ваши замечания помогут мне сделать ее лучше.

В России зачастую предпочитают не покупать книги, а качать из Интернета их пиратские копии, что наносит ущерб и авторам, и издательствам. Доход от книг падает, и многие хорошие авторы перестают писать, ибо настоящему специалисту легко найти достойный источник дохода без лишних мучений. От этого количество хороших книг уменьшается. Боюсь, эта тенденция сохранится.

Если вы нашли в книге какую-нибудь ошибку, просьба сообщить мне об этом через обратную связь на моем сайте **www.flenov.info**. Ошибки могут быть везде, и не только в программах или ОС, но и в текстах книг. Я также жду ваших отзывов о книге и пожеланий, что вы хотите увидеть в ней в будущем, если появится новое издание.

На этом завершаем вступительное слово и переходим к наиболее интересной и главной части книги — знакомству с ОС Linux.

Приятного чтения!

ГЛАВА 1

Прежде чем начать...

Много лет назад установка ОС Linux была очень сложной, и далеко не на каждый компьютер систему удавалось установить, — постоянно возникали проблемы с совместимостью, отсутствием драйверов. Впрочем, такие проблемы были даже у Windows 95, которая так же работала с минимальными функциями, пока на нее не поставят необходимые драйверы.

У меня в 1990-х годах были не очень популярный монитор Philips и специфичная видеокарта, которая отсутствовала в списке доступного оборудования, поэтому мне приходилось подбирать подходящие драйверы из тех, что были в наличии для других систем, чтобы рабочий стол отображался на экране в приемлемом разрешении.

Сейчас установка Linux стала настолько простой, что в некоторых дистрибутивах для полной установки надо всего-то несколько раз щелкнуть мышью — все имеющееся оборудование определяется без проблем и устанавливается без необходимости подбирать драйверы.

Если смотреть на ОС Linux с точки зрения пользователя, то после установки системы ничего настраивать не надо, — можно сразу же приступать к работе с любыми офисными приложениями и пользовательскими утилитами. Дистрибутивы для домашних компьютеров очень часто уже включают и офисные пакеты, и все необходимое на все случаи жизни.

Но если речь идет о сетевых и серверных программах, то тут уже необходимы дополнительные действия. По умолчанию в системе должны быть запрещены практически все действия, которые могут привести к нежелательному результату или вторжению по сети. Для изменения ограничений нужно настраивать конфигурационные файлы, редактировать которые крайне неудобно новичку или пользователю, привыкшему работать с окнами, а также использовать специализированные утилиты, большинство из которых имеют интерфейс командной строки.

Из-за этих неудобств мой знакомый администратор Windows-систем сказал: «Linux придумали администраторы, которым нечего делать на работе, для того, чтобы играться с конфигурационными файлами». Смешно... Но я с этим не согласен, поскольку заглядываю в конфигурационные файлы своих серверов очень редко.

Корпорация Microsoft начинала делать свои ОС по принципу «лишь бы было удобно», поэтому когда-то достаточно было лишь подключить к ним требуемые компоненты. Но теперь Windows становится с каждым годом все сложнее и безопаснее, а большинство удобных функций, которые могут нарушить защиту, просто отключаются. При необходимости их нужно включать. Начиная с 2008 года, эта тенденция приняла совершенно новый и интересный оборот — в Windows Server появилась версия без графического режима. Да, Windows запускается в текстовом режиме, в котором можно полноценно управлять сервером! В Linux все было наоборот — эту ОС создавали с точки зрения «лишь бы было безопасно», а теперь двигаются в сторону наращивания возможностей и упрощения сервисов. Эта тенденция радует не всегда: в некоторых дистрибутивах Linux, если установить какой-либо сервис, то инсталлятор мало того, что устанавливает сервис в максимальной конфигурации, он еще и запускает его автоматически при старте системы. Это очень плохо, и такие вещи нужно пресекать.

Что ж, удобство и безопасность во многом противоречат друг другу, поэтому производителям приходится в чем-то лавировать.

1.1. Ядро

Ядро — это сердце ОС, в котором реализовано управление памятью и другими ресурсами компьютера. Помимо этого, оно позволяет получить доступ к различному «железу». Например, ранние версии ядра обеспечивали работу только двух USB-устройств: клавиатуры и мыши. Современное ядро поддерживает большинство существующих устройств, а дистрибутивы включают драйверы для большинства популярного оборудования.

Номер версии ядра Linux состоит из трех чисел (последнее указывается не всегда):

- первое число — старший номер, который указывает на значительные изменения в ядре;
- второе — младший номер, увеличение которого указывает на появление небольших изменений. По нему можно определить, является ядро проверенным или предназначено для тестирования, когда нет уверенности, что оно не содержит ошибок. Если число четное, то ядро прошло тщательное тестирование. В противном случае установка этой версии не гарантирует стабильной работы;
- третье число — сборка, т. е. номер очередного рабочего релиза. В некоторых случаях это число опускают, ибо оно несет не такую значительную смысловую нагрузку, как предыдущие числа. Например, часто говорят о версии 2.6, и в этом случае не указана именно сборка.

Новые версии ядра можно скачать по адресу **www.kernel.org** или с сайта производителя вашего дистрибутива в виде обновления для самой ОС. Обновление ядра позволяет не только получить новые возможности по работе с «железом» и повысить производительность системы, но и исправить некоторые ошибки. Самое главное, что обновление ядра в Linux не влечет за собой переконфигурирования всей

ОС, как это происходит в некоторых других системах. Я видел компьютеры, ОС которых были установлены еще несколько лет назад и не перенастраивались с тех пор, — в них только обновлялось ядро и программное обеспечение. Такое бывает редко, потому что, как правило, периодически приходится обновлять «железо», наращивая мощности, — ведь запросы программ и пользователей растут не по дням, а по часам.

1.2. Дистрибутивы

В настоящее время существует множество различных дистрибутивов Linux, но между ними легко проглядывается сходство, т. к. большинство имеет общие корни. Например, многие дистрибутивы построены на основе Red Hat Linux. Компании-производители вносят некоторые коррективы в процедуру инсталляции (чаще всего только графические), изменяют список включаемого программного обеспечения и продают под своей маркой. При этом ядро системы и устанавливаемые программы чаще всего поставляются абсолютно без изменений.

Даже если установочные версии имеют разных производителей, в качестве графической оболочки очень часто используется KDE или/и GNOME, а при отсутствии в поставке их всегда можно установить дополнительно. Таким образом, вне зависимости от основного дистрибутива у всех будет одинаковый графический интерфейс.

Еще недавно можно было встретить Unity — оболочку по умолчанию для Ubuntu, но от ее разработки отказались, и дистрибутив снова возвращается к своим корням — GNOME.

Я долго не мог решить, какой дистрибутив установить, но потом решил выбрать Ubuntu. Я заглянул на пару сайтов, посвященных Linux, и посмотрел в статистике перечень операционных систем, с которых заходили на сайт пользователи (такую статистику предоставляет счетчик **mail.ru**). Наиболее популярной оказалась Ubuntu. В принципе, зная один дистрибутив, очень легко перейти на другой, ведь каждый из них — та же Linux.

И все же, на мой взгляд, разнообразие дистрибутивов является самым слабым звеном Linux. Когда вы начнете работать с ней, то увидите, что большая часть операций не стандартизирована (это можно расценивать как следствие открытости кода). Получается как в поговорке: «Кто в лес, кто по дрова». Это серьезная проблема, которая усложняет восприятие. Но в реальности в 99% случаев в дистрибутивах все идентично.

На мой взгляд, неудобство от разнообразия дистрибутивов заключается в том, что производителям приходится много топтаться на месте и писать один и тот же код. Лучше бы они объединились и начали быстрее двигаться вперед. Да, пострадает конкуренция и возможность выбора, но развитие станет намного эффективнее.

В этом смысле ОС Windows более унифицирована и проще для обучения, хотя в последнее время и здесь наблюдается отступление от установленных канонов. Так, внешний вид программ стал совершенно непредсказуем. Меню и панели

в Office 2000, XP, 2003, 2007, 2010, 2013 постоянно изменяются — только успевай к ним привыкать! В Linux, несмотря на отсутствие стандартов, элементы интерфейса пока везде остаются одинаковыми.

Какой дистрибутив выбрать? Их слишком много, чтобы упоминать все, и я остановлюсь только на самых популярных:

- Red Hat Enterprise Linux и SUSE — выбираем, если нужна хорошая корпоративная поддержка;
- CentOS или Debian — чаще выбирают для серверов, когда не нужна дорогая поддержка со стороны производителя;
- Mint, Ubuntu — хороший выбор для домашнего компьютера, если не нужна поддержка;
- Kali — прославился хорошим набором для хакеров и специалистов в области безопасности.

А теперь о некоторых из них немного подробнее.

1.2.1. Red Hat Linux

Этот дистрибутив считается классическим и является законодателем моды в развитии ОС. Помимо всего прочего, Red Hat ведет разработку ОС Linux в двух направлениях: для серверных решений и для клиентских компьютеров. Серверный вариант — платный, а клиентский вариант (Fedora) бесплатен и доступен для скачивания с сайта **fedoraproject.org**. Шли разговоры о том, что Fedora будет независимым проектом, но пока он остался под крылом Red Hat.

Дистрибутивы Linux всегда ругают за сложность установки ядра и программ, которые чаще всего поставляются в исходных кодах и требуют компиляции. Компания Red Hat уже давно упростила этот процесс, разработав менеджер пакетов RPM (Redhat Package Manager). Такие пакеты для установки используют и большинство других разработчиков.

1.2.2. Slackware

Мое знакомство с Linux начиналось именно с дистрибутива Slackware (**www.slackware.com**). Это один из самых старых и сложных для домашних пользователей дистрибутивов. У него до сих пор нет удобной программы установки, и большинство действий приходится делать в текстовом режиме. Конечно же, вы можете добавить к этому дистрибутиву графические оболочки KDE или GNOME, а также другие пакеты, облегчающие работу, но установку проще не сделаешь.

У проекта Slackware даже сайт невероятно простой, и на момент подготовки этого издания он просто черно-белый с минимальным использованием графики.

Если вы ни разу не работали с Linux, то я бы не рекомендовал начинать знакомство с этого дистрибутива. Лучше выбрать что-нибудь попроще.

1.2.3. SuSE Linux

Мне приходилось работать с разными программами от немецких производителей, но удобство работы с ними не просто хромало, а создавалось впечатление, что эти программы — безногие калеки с детства. Однако разработка от SuSE (**www.suse.com**) опровергает такое мнение. Этот дистрибутив отличается симпатичным интерфейсом и отличной поддержкой оборудования, потому что содержит громадную базу драйверов. Кроме того, программисты SuSE добавили в дистрибутив набор утилит под названием YaST, которые значительно упрощают администрирование.

SuSE Linux — наверное, один из первых дистрибутивов, который стал дружественным к пользователю и использует большое количество собственных наработок, чтобы сделать жизнь домашнего пользователя проще. Но при этом он всегда был платным, причем цена очень даже сильно не радовала. Мне кажется, что именно это помешала SuSE занять верхнюю ступень пьедестала и обойти Ubuntu. Сейчас у SuSE Linux есть бесплатная версия — openSUSE, но она пока не набирает популярности.

Я бы посоветовал SuSE только любителям и для использования на клиентских компьютерах. Тем более, что это один из платных дистрибутивов, который распространяется «в коробке».

1.2.4. Debian

Несмотря на то, что цель любого производителя — получение прибыли, существует множество дистрибутивов, которые были и остаются некоммерческими. Основным и самым крупным из них можно считать Debian (**www.debian.org**). Этот продукт создают профессионалы для себя, но пользоваться им может каждый.

ОС Debian имеет больше всего отличий от классической Red Hat, и у вас могут возникнуть проблемы из-за разного расположения некоторых конфигурационных файлов. Но на этом проблемы не заканчиваются. Как и все некоммерческие проекты, этот дистрибутив сложнее других. Разработчики позиционируют Debian как надежную ОС, и это у них получается, а вот о простых пользователях они заботятся мало, поэтому домашние компьютеры этот дистрибутив завоюют не скоро.

1.2.5. Ubuntu

Это, наверное, один из самых простых дистрибутивов, над которым работает компания Canonical Ltd. При его создании основной целью была простота, и, кажется, в 2009 году компания заявила, что в течение двух лет планирует сделать дистрибутив красивее и удобнее macOS. Они видимо хотели это сделать с помощью своей оболочки Unity, которую недавно прикрыли. Сайт разработчиков: **www.ubuntu.com**.

Дистрибутив построен на базе Debian (к сожалению, в одном из предыдущих изданий здесь была допущена ошибка — благодаря приему copy/paste в это место попа-

ло название компании Red Hat). Выбор компании Canonical Ltd. ясен — в лице Debian они выбрали очень безопасную основу. Единственное, что меня пугает, — большинство статистических обзоров показывает, что ежегодно в Ubuntu находят больше уязвимостей, чем в конкурентах. И это при том, что в ОС Debian, на которой основана Ubuntu, уязвимостей находят очень мало.

Статистикам и аналитикам верить очень сложно, особенно с точки зрения безопасности, потому что безопасность измерить невозможно. В дистрибутиве может быть найдена сотня уязвимостей, но он останется надежным, если все они незначительные. С другой стороны, достаточно одной уязвимости, но очень серьезной, которую можно легко использовать и которую залатают с большим опозданием, чтобы надежность опустилась до нуля.

1.2.6. Raspbian

Это еще одна ОС, построенная на Debian, но ее основное назначение — устройства IoT (Internet of Things, или Интернет вещей). И основное место использования этой ОС — на одноплатном компьютере Raspberry PI.