Оглавление

ПРЕДИСЛОВИЕ 13

Так для кого эта книга 14
От издательства 14
Благодарности 15

ГЛАВА 1. СВЯЗИ 16

1.1. Канальный уровень 17
Общие связи 18
MAC-адресация 21
Кадры 24
1.2. Межсетевой уровень 25
Межсетевое взаимодействие 28
Маршрутизация 28
Адресация местоположения 30
Интернет-протокол 31
1.3. IP-адресация 33
IANA 35
Провайдеры интернет-услуг 37
1.4. IP-маршрутизация 39
Таблицы адресов 40
Точки обмена интернет-трафиком 43
Интернет-магистраль 44
Динамическая маршрутизация 44
Петля маршрутизации 45
Диагностика 47
1.5. Транспортный уровень 50
Протокол пользовательских дейтаграмм 50
Протокол управления передачей данных 53

Сегменты TCP 54
TCP-соединение 57
TCP-сокеты 59
Резюме 60
Дополнительная информация. 62

ГЛАВА 2. ОБМЕН ДАННЫМИ 63

2.1. Имена. 64
Домены 64
ICANN 65
Серверы имен 66
Запрос 67
Рекурсивный запрос 69
Типы записей 70
Обратный DNS-запрос. 72
Регистрация домена 73
2.2. Время. 75
Координированное универсальное время 76
Протокол сетевого времени 78
Серверы времени. 80
2.3. Доступ 82
Терминалы. 82
Telnet 85
2.4. Почта 86
Почтовые серверы 87
Simple Mail Transfer Protocol 88
Отправка электронных писем. 91
Получение электронных писем. 93
2.5. Сеть 94
Язык разметки гипертекста. 95
URL-адрес 97
Протокол передачи гипертекста 99
Веб-приложения 101

Резюме 103
Номера портов 103
Одноранговое соединение 104
Безопасность 104
Дополнительная информация 105

ГЛАВА 3. БЕЗОПАСНОСТЬ 106

3.1. Устаревшие шифры 107
Зигзагообразный шифр 108
Шифр подстановки 109
Продукционные шифры 111
Шифр Виженера 112
Шифр Вернама 113
Шифровальные машины 115
3.2. Симметричные шифры 116
Потоковые шифры 117
Блочные шифры 120
3.3. Асимметричные шифры 124
Обмен ключами Диффи — Хеллмана 125
Шифры с открытым ключом 126
Цифровые подписи 127
Цифровые сертификаты 128
3.4. Хеширование 129
Обнаружение злонамеренных изменений 130
Код аутентификации сообщения 131
Обработка паролей 132
Доказательство существования 134
Подтверждение работы 135
Небезопасные хеш-функции 136
3.5. Протоколы 137
Безопасный доступ 138
Безопасная передача 139
Другие протоколы 140

3.6. Хакинг 141
Социальная инженерия 142
Уязвимости программного обеспечения 145
Эксплойты 148
Цифровая война 150
Чек-лист защиты 152
Резюме 153
Дополнительная информация. 154

ГЛАВА 4. АНАЛИЗ ДАННЫХ. 155
Сбор данных. 156
4.1. Сбор. 158
Виды данных 158
Получение данных 159
Ошибка выборки 161
4.2. Обработка 162
Первичная очистка данных 162
Анонимизация данных 167
Воспроизводимость 168
4.3. Обобщение 170
Количество 170
Средние значения 170
Изменчивость. 172
Сводка пяти чисел 173
Категориальное обобщение 176
Корреляционная матрица. 176
4.4. Визуализация 179
Ящик с усами 180
Гистограммы 182
Точечные диаграммы 186
Временные ряды 190
Карты. 194
4.5. Тестирование 195
Гипотезы. 195

Эксперименты 198
P-значения 200
Доверительные интервалы 202
Резюме 203
Дополнительная информация 205

ГЛАВА 5. МАШИННОЕ ОБУЧЕНИЕ 206
Модели 207
5.1. Признаки 210
Адаптация данных 211
Объединение данных 216
Пропущенные значения 218
Утечка данных 221
5.2. Оценка 223
Оценка регрессоров 225
5.3. Проверка работоспособности 227
K-folds 229
Монте-Карло 231
Исключение по одному (leave-one-out) 232
Интерпретация 232
5.4. Подстройка 233
Подстановка 235
Выбросы 235
Нормализация 236
Логарифмическое преобразование 237
Биннинг 238
Кластеризация 238
Извлечение признаков 239
Отбор признаков 242
И снова утечка данных 243
Выбор модели 244
Заключительные шаги 245
Резюме 246
Дополнительная информация 248

ЗАКЛЮЧЕНИЕ. 249

БОНУСНАЯ ГЛАВА 6. ШАБЛОНЫ 251

6.1. Соответствие 253
Точка 253
Множество. 254
Обратное множество. 256
Специальные символы 257

6.2. Квантификаторы 258
Фигурные скобки. 258
Вопрос 259
Плюс 260
Звездочка 260
Жадность 261

6.3. Привязки. 262
Каретка. 262
Доллар. 262
Граница 263

6.4. Группы 264
Захват групп. 265
Чередование 266

Резюме 267

Дополнительная информация. 269

ПРИЛОЖЕНИЯ 270

I. Основания систем счисления 270

II. Взлом шифра сдвига. 271

III. Взлом шифра подстановки. 272

IV. Оценка классификаторов. 274
Компромисс в классификации 279
Кривые ROC 280
Многоклассовая классификация. 282