

# Оглавление

ПРЕДИСЛОВИЕ .....	2
<b>Глава 1 СЕТЕВЫЕ АНОМАЛИИ, МЕТОДЫ, СИСТЕМЫ И ИНСТРУМЕНТЫ АНАЛИЗА .....</b>	<b>7</b>
1.1. Типы и классификация аномалий .....	7
1.1.1. Классификации аномалий .....	7
1.1.2. Аномалии временных последовательностей .....	9
1.1.3. Аномалии производительности и изменения приложений .....	10
1.2. Методы обнаружения сетевых аномалий .....	11
1.2.1. Поведенческие методы .....	12
1.2.2. Методы машинного обучения .....	15
1.2.3. Методы вычислительного интеллекта .....	18
1.2.4. Методы основанные на знаниях .....	21
1.3. Обнаружение аномалий в потоковых данных .....	25
1.3.1. Формулировки задачи и сценарии обнаружения аномалий в дискретных последовательностях .....	25
1.3.2. Обнаружение аномальных временных рядов относительно базы данных временных рядов. Секвенциальный анализ темпоральных данных .....	27
1.3.3. Обнаружение аномальных последовательностей в потоке данных на основе знаний о цепочке событий, произошедших ранее в данном потоке .....	29
1.3.4. Обнаружение аномальных паттернов на основе анализа частоты их появления .....	29
1.3.5. Обнаружение аномалий в реальном времени .....	30
1.4. Системы и инструменты обнаружения сетевых аномалий .....	31
1.4.1. Типы сетевых аномалий .....	31
1.4.2. Классификация методов и систем обнаружения сетевых аномалий .....	33
1.4.3. Обнаружение сетевых аномалий .....	35
1.4.4. Существенные аспекты обнаружения сетевых аномалий .....	38
1.4.5. Обучающие выборки для задачи обнаружения аномалий .....	44
1.5. Метрики, используемые для оценки методов и систем обнаружения сетевых аномалий .....	45
1.5.1. Оценка эффективности алгоритмов обнаружения .....	45
1.5.2. Оценка эффективности алгоритмов классификации и кластеризации .....	

Литература к главе 1 .....	51
<b>Глава 2. АНАЛИЗ И МОНИТОРИНГ СЕТЕВОГО ТРАФИКА</b> .....	<b>55</b>
2.1. Проблемы контроля и анализа сетевого трафика .....	55
2.1.1. Место контроля трафика .....	56
2.1.2. Задачи контроля .....	57
2.2. Сетевые анализаторы трафика .....	59
2.2.1. Задачи анализа сетевого трафика .....	59
2.2.2. Средства анализа сетевого трафика .....	60
2.2.3. Программный сниффер Wireshark .....	64
2.2.4. Аппаратный сниффер Network Associates .....	66
2.2.5. Iris Network Traffic Analyzer .....	66
2.3. Сбор данных с помощью протокола NetFlow .....	67
2.3.1. Мониторинг .....	67
2.3.2. Примеры контрольных и аналитических инструментов потока сетевого трафика с помощью протокола NetFlow .....	68
2.4. Сбор данных с помощью протокола SNMP .....	70
2.4.1. Контроль сетевых устройств .....	70
2.4.2. Примеры контрольных и аналитических инструментов потока сетевого трафика помощью протокола SNMP .....	71
2.5. Программный сниффер Tsrdump .....	72
2.6. Другие технологии и подходы к сетевому мониторингу .....	74
2.6.1. Трассировка событий сетевого стека .....	74
2.6.2. Протокол ICMP .....	74
2.6.3. Анализ системных журналов .....	75
2.7. Инструменты классификации. Технология DPI .....	75
2.8. Использование инструментов DPI для классификации и учета трафика .....	78
2.8.1. Использование инструментов DPI для классификации трафика .....	78
2.8.2. Использование инструментов DPI для целей учета тра- фика .....	79
2.8.3. Влияние усечения пакетов и потоков на классификацию трафика .....	80
2.9. Наборы обучающих и тестовых данных обнаружения сетевых атак .....	81
2.9.1. Синтетические данные .....	81
2.9.2. Эталонные данные .....	82
2.9.3. Реальные наборы данных .....	87
2.9.4. Симуляция сети .....	89
2.10. Системы и инструменты для анализа потоковых данных .....	90
Литература к главе 2 .....	97

<b>Глава 3. СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ СЕТЕВЫХ АНОМАЛИЙ</b> .....	100
3.1. Аномалии сетевой безопасности .....	100
3.1.1. Типы сетевых атак .....	101
3.1.2. Примеры формирования атакующего трафика.....	101
3.2. Примеры сетевых атак полученные имитационным моделированием аномалий трафика в локальной сети .....	112
3.3. Статистические характеристики трафика с DoS-атакой .....	114
3.3.1. ICMP flooding .....	114
3.3.2. Flash crowd.....	117
3.3.3. Smurf .....	119
3.3.4. Fraggle.....	120
3.3.5. SYN flooding .....	120
3.3.6. UDP storm .....	121
3.4. Анализ статистических характеристик используемых для описания аномальных вторжений .....	121
3.5. Результаты анализа статистических характеристик аномальных вторжений .....	124
3.5.1. Атака Flash crowd.....	124
3.5.2. Атака ICMP flooding.....	126
3.5.3. Атака fraggle.....	128
3.5.4. Атака smurf.....	130
3.5.5. Атака SYN flooding .....	132
3.5.6. Атака UDP storm .....	134
3.5.7. Neptune .....	136
3.6. Информативные статистические параметры аномальных вторжений.....	137
3.7. Классификация аномальных вторжений статистическими методами .....	141
3.7.1. Методы классификации .....	141
3.7.2. Результаты классификации аномалий на основе оценки статистических параметров .....	144
3.8. Фрактальные свойства телекоммуникационного трафика .....	148
Литература к главе 3 .....	152
<b>Глава 4. СТАТИСТИЧЕСКИЕ МЕТОДЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ</b> .....	154
4.1. Статистические методы обнаружения аномального поведения .....	154
4.1.1. Принципы статистических методов обнаружения аномалий.....	154
4.1.2. Классификация методов обнаружения.....	157
4.2. Критерии соответствия и однородности .....	159
4.2.1. Критерий хи-квадрат.....	159

4.2.2. Критерий Колмогорова–Смирнова.....	160
4.2.3. Критерий оценки Вилкоксона–Манна–Уитни.....	161
4.3. Критерии аномального поведения и их практическое применение.....	162
4.3.1. Признаки появления аномалии.....	162
4.3.2. Процентное отклонение (PD).....	163
4.4. Параметрические методы регистрации изменений.....	165
4.4.1. Контрольные карты.....	166
4.4.2. Контрольные карты Шухарта.....	167
4.4.3. Контрольные карты CUSUM.....	168
4.4.4. Контрольные карты EWMA.....	169
4.5. Статистические алгоритмы и методы идентификации аномалий.....	170
4.5.1. Алгоритм обобщенных экстремальных отклонений.....	170
4.5.2. Алгоритм обнаружения выбросов на основе вычисления эксцесса.....	171
4.5.3. Алгоритм Шапиро–Вилка.....	171
4.5.4. Алгоритм обнаружения нескольких выбросов отличающихся различными параметрами.....	171
4.5.5. Алгоритм обнаружения одного выброса в упорядоченной выборке.....	172
4.5.6. Алгоритм идентификации выбросов, основанный на экспоненциальном сглаживании.....	173
4.5.7. Алгоритм оценки соответствия новых входных данных наблюдений уже имеющимся.....	173
4.5.8. Алгоритм фильтрующего окна.....	174
4.5.9. Матричные методы обнаружения выбросов.....	174
4.6. Методы, критерии и алгоритмы математической статистики ..	175
4.6.1. Методы описательной статистики.....	175
4.6.2. Критерий Кохрана–Кокса.....	177
4.6.3. Критерий Беренса–Фишера сравнения выборок при неизвестных неравных дисперсиях.....	178
4.6.4. Критерий сравнения двух параметров экспоненциальных распределений.....	178
4.6.5. Критерий Фишера для дисперсий.....	179
4.6.6. Композиция статистических критериев для работы в режиме on-line.....	179
4.7. Сравнительный анализ алгоритмов обнаружения аномалий статистическими методами в режиме on-line.....	181
4.7.1. Постановка задачи.....	181
4.7.2. Численные результаты обнаружения аномалий в режиме on-line.....	182
4.8. Обнаружение аномальных выбросов с использованием информационных критериев.....	189

4.8.1. Методика обнаружения .....	189
4.8.2. Численные результаты .....	190
4.9. Обнаружение аномалий трафика с использованием алгоритма кумулятивных сумм .....	194
4.9.1. Структура алгоритма .....	194
4.9.2. Описание алгоритма обнаружения .....	195
4.9.3. Численные результаты .....	197
4.10. Обнаружение и оценка момента возникновения сетевых аномалий методом разладки Бродского–Дарховского .....	202
4.10.1. Постановка задачи .....	202
4.10.2. Критерии обнаружения .....	203
4.10.3. Алгоритм Бродского–Дарховского .....	203
4.10.4. Результаты статистической обработки с использованием алгоритма Бродского–Дарховского .....	205
4.11. Поиск и оценка аномалий сетевого трафика на основе циклического анализа .....	207
4.12. Информационно-теоретические модели обнаружения аномалий .....	214
4.13. Обнаружение аномальных вторжений с помощью модели смеси гауссовских распределений .....	218
4.14. Применение сэмплинга трафика для систем мониторинга рисков безопасности в IP-сетях .....	220
4.14.1. Технология выборки и анализа трафика в IP-сетях .....	220
4.14.2. Методы сэмплинга .....	222
4.14.3. Механизм реализации адаптивного сэмплинга на сетевом устройстве .....	224
4.14.4. Адаптация частоты дискретизации путем удаленного доступа .....	225
4.14.5. Примеры применения сэмплинга для обнаружения сетевых аномалий .....	227
4.15. Достоинства и недостатки статистических методов .....	230
Литература к главе 4 .....	232
<b>Глава 5. ОБНАРУЖЕНИЕ АНОМАЛИЙ ТРАФИКА МЕТОДАМИ КРАТНОМАСШТАБНОГО АНАЛИЗА .....</b>	<b>235</b>
5.1. Основные положения кратномасштабного анализа (КМА) .....	235
5.2. Обнаружение аномалий трафика с помощью вейвлет-анализа .....	238
5.2.1. Непрерывное вейвлет-преобразование .....	240
5.2.2. Дискретные вейвлет-преобразования: разложение и реконструкция .....	241
5.2.3. Дискретное вейвлет-преобразование с максимальным перекрытием .....	243
5.2.4. Пакетные вейвлеты .....	245

5.3. Анализ методов обнаружения аномалий трафика с помощью вейвлетов .....	246
5.3.1. Качественный анализ .....	246
5.3.2. Обнаружение DDoS-атак на основе оценки энергии коэффициентов детализации дискретного вейвлет-преобразования .....	249
5.3.3. Обнаружение на основе пакетных вейвлетов .....	250
5.3.4. Критерии выбора вейвлет-функции .....	251
5.4. Обнаружение аномалий методами ДВП в режиме off-line .....	253
5.4.1. Статистические характеристики коэффициентов аппроксимации и детализации .....	253
5.4.2. Алгоритм, основанный на сумме квадратов вейвлет-коэффициентов .....	254
5.4.3. Алгоритм, основанный на максимуме квадратов вейвлет-коэффициентов .....	257
5.4.4. Сравнительный анализ алгоритмов обнаружения .....	260
5.5. Обнаружение аномалий методами ДВП в режиме on-line .....	261
5.5.1. Статистические характеристики аномалии .....	261
5.5.2. Алгоритмы обнаружения .....	265
5.5.3. Результаты статистической обработки .....	267
5.6. Обнаружение аномалий методами ДВП в режиме on-line с учетом предварительной фильтрации .....	270
5.6.1. Предварительная фильтрация трафика методами трешолдинга .....	270
5.6.2. Оценка эффективности трешолдинга при обнаружении аномалий .....	271
5.6.3. Результаты статистической обработки аномально засоренного трафика .....	275
5.7. Оценка достоверности обнаружения аномалий методами кратномасштабного анализа .....	277
5.7.1. Оценка вероятностных характеристик достоверности обнаружения при использовании критерия Фишера .....	277
5.7.2. Оценка вероятностных характеристик достоверности обнаружения при использовании критерия Фишера для средних значений .....	280
5.7.3. Структура программного комплекса .....	282
5.7.4. Сравнительный анализ результатов обнаружения аномалий при использовании различных длительностей окон анализа .....	285
5.7.5. Сравнительный анализ результатов обнаружения аномалий при использовании различных систем вейвлетов .....	286
Литература к главе 5 .....	289

<b>Глава 6. ОБНАРУЖЕНИЕ АНОМАЛИЙ МЕТОДАМИ МОНО И МУЛЬТИФРАКТАЛЬНОГО АНАЛИЗА.....</b>	<b>291</b>
6.1. Основные положения теории фракталов и мультифракталов ..	291
6.2. Мультифрактальный анализ трафика методом максимумов модулей вейвлет-преобразования .....	296
6.2.1. Особенности определения спектра сингулярностей мультифрактального сигнала .....	296
6.2.2. Алгоритм оценки параметров мультифрактального спектра методом ММВП .....	298
6.3. Имитационное моделирование мультифрактальных характеристик телекоммуникационного трафика в условиях DoS-атак ....	299
6.4. Обнаружение аномалий методом мультифрактального кратномасштабного анализа в реальном времени .....	308
6.4.1. Постановка задачи .....	308
6.4.2. Метод оценки скачка фрактальной размерности в режиме on-line .....	309
6.4.3. Эффективность текущей оценки показателя Херста .....	312
6.4.4. Мультифрактальное расширение алгоритма обработки ..	313
6.4.5. Результаты эксперимента .....	313
6.4.6. Анализ полученных результатов .....	316
6.5. Оценка показателя Херста методом кратномасштабного анализа	318
6.6. Анализ методов оценки монофрактальной размерности .....	320
6.6.1. Методы оценки показателя Херста.....	320
6.6.2. Алгоритмы оценки параметров самоподобия .....	321
6.6.3. Итеративный алгоритм оценки показателя Херста.....	322
6.6.4. Упрощенная процедура оценки показателя Херста.....	323
6.6.5. Оценка показателя Херста на основе вейвлет-анализа ...	325
6.6.6. Алгоритм обнаружения аномалий на основе дискретного стационарного вейвлет-преобразования (DSWT) и фрактальной размерности (FD) .....	326
6.7. Примеры обнаружения аномалий сетевого трафика методом оценки фрактальной размерности .....	327
6.7.1. Обнаружение аномалий в сетевом трафике локальной сети методом оценки самоподобия .....	327
6.7.2. Оценка уровня риска безопасности LAN на основе оценки самоподобия трафика.....	331
6.7.3. Обнаружения атаки DDoS Flood с помощью ДВП и SIC	334
Литература к главе 6 .....	336
<b>Глава 7. СЕТЕВАЯ ТОМОГРАФИЯ. ОБНАРУЖЕНИЕ И ЛОКАЛИЗАЦИЯ АНОМАЛИЙ ОБЪЕМА .....</b>	<b>339</b>
7.1. Основные положения сетевой томографии .....	339

7.2. Обнаружение и локализация аномалий в крупномасштабных сетях .....	342
7.3. Систематизация аномалий объема сети .....	345
7.4. Моделирование и оценка матрицы трафика .....	347
7.5. Оценка ТМ .....	350
7.5.1. Информационно-теоретический подход к оценке ТМ ....	350
7.5.2. Некорректные обратные задачи .....	352
7.6. Оценка ТМ методом максимального правдоподобия .....	354
7.6.1. Модель самоподобного трафика .....	355
7.6.2. Функция правдоподобия .....	358
7.7. Рекуррентная оценка матрицы трафика .....	363
7.8. Оценка ТМ методом главных компонент .....	365
7.9. Методы обнаружения и локализации аномалий объема .....	368
7.9.1. Обнаружение аномалий с использованием фильтра Калмана .....	368
7.9.2. Обнаружение и локализаций аномалий методом РСА ...	369
7.9.3. Результаты имитационного моделирования .....	371
7.10. Структура системы мониторинга аномалий объема в больших распределенных системах .....	377
Литература к главе 7 .....	379
<b>Глава 8. ОБНАРУЖЕНИЕ И ПРОГНОЗИРОВАНИЕ АНОМАЛИЙ В ПОТОКОВЫХ ДАННЫХ .....</b>	<b>382</b>
8.1. Обнаружение аномалий на основе прогнозирования профиля нормального функционирования .....	382
8.1.1. Профиль нормального функционирования .....	382
8.1.2. Краткосрочное прогнозирование временных рядов .....	383
8.2. Анализ существующих методов прогнозирования .....	385
8.2.1. Основные понятия и определения .....	385
8.2.2. Обнаружение аномалий с помощью экспоненциального сглаживания временного ряда. Глубина упреждения прогноза .....	386
8.2.3. Статистические модели прогнозирования .....	387
8.3. Регрессионные модели .....	391
8.3.1. Линейные авторегрессионные (AR) модели .....	392
8.3.2. Процессы скользящего среднего .....	393
8.3.3. Авторегрессионные модели скользящего среднего .....	393
8.3.4. Авторегрессионные интегральные модели скользящего среднего (ARIMA) .....	395
8.3.5. Фрактальные авторегрессионные интегральные модели скользящего среднего (FARIMA) .....	396
8.3.6. Выбор порядка AP-модели .....	397

8.4. Этапы обнаружения аномалий объектов мониторинга с помощью ПНФ .....	400
8.5. Обнаружение аномалий в потоках данных временных рядов ...	402
8.5.1. Модели потоков данных .....	402
8.5.2. Факторы, влияющие на выбор метода обнаружения аномалий .....	404
8.5.3. Подходы к обнаружению аномалий в потоковых данных	406
8.6. Методы и алгоритмы обнаружения аномалий в потоковых данных .....	408
8.6.1. Анализ экстремальных значений .....	408
8.6.2. Тест Граббса .....	410
8.6.3. Тест обобщенных экстремальных отклонений .....	410
8.6.4. Простая линейная регрессия .....	411
8.6.5. Локальный коэффициент выбросов .....	412
8.7. Обнаружение аномалий в темпоральных данных на основе цепей Маркова .....	413
8.7.1. Дискретные цепи Маркова .....	413
8.7.2. Гибридно продукционно-стохастическая модель .....	416
8.7.3. Марковская модель с доходами .....	417
8.8. Обнаружения аномалий в потоковых данных на основе скрытых марковских моделей .....	419
8.8.1. Основные теоретические положения .....	419
8.8.2. Основные задачи, решаемые с помощью СММ .....	422
8.8.3. Алгоритм метода Баума–Велша обучения СММ системы	423
8.8.4. Алгоритм вычисления состояний СММ методом Витерби	425
8.8.5. Примеры построения и использования СММ в задачах обнаружения аномалий .....	426
8.8.6. Схема обучения СММ .....	429
8.8.7. Прогнозирование сетевых аномалий с помощью СММ ...	431
8.8.8. Преимущества и недостатки методов, основанных на СММ .....	434
Литература к главе 8 .....	434