

Оглавление

Предисловие	3
1. Классические парадигмы машинного обучения и интеллектуального анализа данных	6
1.1. Основные понятия. Технологии KDD и Data Mining....	6
1.2. Методы обнаружения и классификации компьютерных атак и сетевых аномалий методами ИИ	12
1.2.1. Классификация методов обнаружения компьютерных атак и сетевых аномалий	12
1.2.2. Поведенческие методы	13
1.2.3. Методы основанные на знаниях	16
1.2.4. Методы вычислительного интеллекта	17
1.2.5. Методы машинного обучения	19
1.3. Классические методы МО	21
1.3.1. Алгоритмы классификации	21
1.3.2. Нейронные сети и глубокое обучение	22
1.4. Обучение с подкреплением	25
1.5. Визуализация и алгоритмы понижения размерности ...	27
1.5.1. Метод главных компонент	28
1.5.2. Линейное многомерное масштабирование	30
1.5.3. Isomap	31
1.5.4. Стохастическое вложение соседей с t-распределением ..	32
1.6. Ассоциативный анализ	34
1.6.1. Основные понятия	34
1.6.2. Алгоритм APRIORI	35
1.6.3. Алгоритм FP-GROWTH	37
1.7. Методы поиска паттернов в последовательности событий для прогнозирования аномальных событий КС	37
1.7.1. Выделение закономерностей	37
1.7.2. Секвенциальный анализ	39
1.8. Системы и инструменты обнаружения сетевых атак	40
1.8.1. Типы сетевых атак	40
1.8.2. Классификация методов и систем обнаружения сетевых атак	42
1.8.3. Обнаружение сетевых аномалий	44

Литература.....	44
2. Классификация. Обучение с учителем	48
2.1. Математическая постановка задачи классификации	48
2.2. Линейный классификатор	48
2.2.1. Бинарная и многоклассовая линейная классификация	48
2.2.2. Логистическая регрессия	50
2.2.3. Байесовский классификатор.....	51
2.2.4. Наивный байесовский классификатор.....	52
2.3. Метод опорных векторов.....	53
2.4. Метрические классификаторы	55
2.4.1. Алгоритм KNN	55
2.4.2. Ближайший центроид	56
2.5. Алгоритмы на основе деревьев решений.....	56
2.5.1. Основные понятия	56
2.5.2. Дерево классификации и регрессии	59
2.5.3. Алгоритм C4.5	60
2.5.4. Алгоритм ID2.....	61
2.5.5. Алгоритм CHAID	62
2.6. Ансамблевые алгоритмы.....	63
2.6.1. Методы композиции обучающихся алгоритмов.....	63
2.6.2. Бустинг.....	64
2.6.3. Бэггинг.....	65
2.6.4. Стекинг.....	66
2.6.5. Случайный лес	67
2.7. Нейронные сети	68
2.7.1. Искусственные нейронные сети	68
2.7.2. Рекуррентные нейронные сети	70
2.7.3. Нейронные сети, использующие архитектуру LSTM ..	71
2.7.4. Управляемые рекуррентные блоки.....	73
2.7.5. Генеративно-состязательные нейронные сети.....	74
2.7.6. Сверточные нейронные сети	75
2.8. Леса решений. Случайный лес.....	78
2.8.1. Основные положения	78
2.8.2. Построение ДР	82
2.8.3. Голосование.....	83
2.9. Таксономия классификатора RF.....	84
2.10. Изолирующий лес.....	90
2.10.1. Идея изолирующего леса.....	90
2.10.2. Этап обучения	92
2.10.3. Этап тестирования	94
2.11. Метод усиления слабых моделей.....	96

2.12. Оценка устойчивости классификатора	97
2.12.1. Метод контрольных	97
2.12.2. Случайные подвыборки	97
2.12.3. Перекрестная проверка	98
2.13. Поточковая классификация	99
2.13.1. Сценарии обработки потоковых данных	100
2.13.2. Дрейф концепта при потоковой классификации	101
2.14. Алгоритмы потоковой классификации	105
2.14.1. Алгоритм Adaptive Random Forest	106
2.14.2. Adaptive windowing (ADWIN)	109
2.14.3. Эволюция алгоритмов потоковой классификации	111
2.14.4. Граница Хёфдинга	112
2.14.5. Деревья Хёфдинга	112
2.14.6. Особенности ПО классификации данных в потоке	113
2.15. Метрики оценки эффективности классификации	113
2.15.1. Метрики оценки эффективности классификации в режиме оффлайн	113
2.15.2. Оценка эффективности потоковых алгоритмов	117
Литература	118
3. Кластеризация. Обучение без учителя	123
3.1. Математическая постановка задачи кластеризации	123
3.2. Методы кластерного анализа данных	124
3.2.1. Иерархические методы	128
3.2.2. Неиерархические методы	134
3.2.3. Сетевые методы	140
3.3. Сравнительный анализ методов кластеризации	145
3.3.1. Параметры сравнения	145
3.3.2. Самоорганизующаяся карта Кохонена	148
3.3.3. Метрики оценки качества алгоритмов кластеризации	152
Литература	155
4 Базы данных аномальных вторжений и сетевых атак	158
4.1. Структура обучающих и тестирующих данных	158
4.2. Набор данных KDD	159
4.2.1. Набор данных NSL-KDD Dataset	160
4.2.2. Временная структура данных KDD	163
4.2.3. Классы в KDD	167
4.3. Набор данных CSIC 2.0 HTTP	169
4.4. Набор данных Enron Dataset	170
4.5. База данных UNSW-NB15	173
4.5.1. Особенности сбора и статистика трафика	173
4.5.2. Предварительная обработка данных	182

4.6. База данных CICIDS 2017.....	198
4.6.1. Архитектура сети.....	198
4.6.2. Профили атак.....	200
4.6.3. Описание набора данных.....	201
4.7. Отбор числа и состава информативных признаков с использованием программных средств.....	204
4.7.1. Особенности отбора признаков в задачах бинарной и многоклассовой классификации.....	204
4.7.2. Использование библиотек языка программирования Python.....	206
4.7.3. Отбор информативных признаков с использованием моделей.....	208
4.7.4. Отбор признаков с использованием статистического подхода.....	209
4.7.5. Сравнительный анализ результатов классификации при различных способах отбора признаков.....	213
4.7.6. Реализация алгоритмов выбора атрибутов в ПО Weka.....	216
Литература.....	219
5. Обнаружение и классификация сетевых атак методами машинного обучения.....	223
5.1. Бинарная классификация атак на примере базы данных UNSW-NB15.....	223
5.1.1. Описание набора данных.....	225
5.1.2. Сравнительный анализ алгоритмов классификации..	227
5.2. Многоклассовая классификация атак на примере базы данных NSL-KDD.....	232
5.2.1. Этапы классификации.....	232
5.2.2. Результаты классификации.....	234
5.3. Сравнительный анализ алгоритмов iForest и Random Forest при бинарной классификации.....	242
5.3.1. Результаты бинарной классификации алгоритма iForest.....	243
5.3.2. Результаты бинарной классификация алгоритма Random Forest.....	245
5.4. Влияние фрактальной размерности на качество бинарной классификации сетевых атак задачи.....	247
5.4.1. Оценка фрактальной размерности.....	249
5.4.2. Результаты бинарной классификации.....	252
5.5. Обнаружение компьютерных атак с применением нейронных сетей.....	258
5.5.1. Этапы обнаружения.....	258
5.5.2. Архитектурные решения COV.....	259
5.5.3. Результаты экспериментов.....	261

5.6. Использование самоорганизующейся карты Кохонена ..	262
5.7. Обнаружение и классификация сетевых аномалий с использованием гибридных искусственных нейронных сетей	269
5.7.1. Анализ результатов синтеза ИНС	272
5.7.2. Анализ результатов классификации атак	274
Литература	277
6. Нечеткая логика в задачах информационной безопасности	280
6.1. Основные теоретические положения нечеткой логики ..	280
6.1.1. Основные понятия и определения	280
6.1.2. Способы нечеткого вывода	281
6.1.3. Формирование базы правил	283
6.1.4. Фаззификация входных переменных	285
6.1.5. Агрегирование степени истинности предпосылок	286
6.1.6. Активация подзаключений	287
6.1.7. Аккумуляция заключений	288
6.1.8. Дефаззификация	289
6.2. Алгоритмы нечеткого вывода	291
6.2.1. Алгоритм Мамдани	291
6.2.2. Метод нечёткого вывода Такаги–Сугено	292
6.3. Примеры реализации алгоритмов нечеткой классификации в задачах ИБ	293
6.3.1. Нечеткая классификация	293
6.3.2. Стратегия формирования нечетких правил	294
6.3.3. Классификация с использованием нечёткой логики Такаги–Сугено	298
Литература	305
7. Искусственные иммунные системы в информационной безопасности	307
7.1. Базовые принципы искусственных иммунных систем. Принцип действия иммунной системы человека	307
7.1.1. Основные свойства иммунной системы человека	307
7.1.2. Негативный и положительный отбор. Лимфоциты, антигены, геновая библиотека, негативная селекция	308
7.1.3. Клональная селекция	311
7.1.4. ИИС на основе гиперклеток	312
7.1.5. Иммунные сети	313
7.1.6. Иммунный ответ	315
7.1.7. Комбинирование методов	316

7.2. Области и подходы применения ИИС в системах информационной безопасности	316
7.2.1. Цели работы ИИС	316
7.2.2. Задачи, решаемые ИИС	316
7.2.3. Классификация методов искусственных иммунных систем	319
7.2.4. Архитектура искусственной иммунной системы	320
7.3. Применение ИИС для обнаружения сетевых аномалий	321
7.3.1. Особенности применения ИИС в системах сетевой безопасности. Схема иммунной системы обнаружения компьютерных атак	321
7.3.2. Эволюция геной библиотеки	323
7.3.3. Создание пре-детекторов, автоматическое профилирование	325
7.3.4. Обнаружение аномалий методами клональной селекции	326
7.3.5. Алгоритмы метода иммунного ответа. Применение систем противодействия компьютерным атакам на основе метода иммунного ответа	327
7.3.6. Обзор существующих реализаций ИИС в области сетевой безопасности	330
7.4. СОА на основе иммунного ответа с нейросетевыми детекторами	335
7.4.1. Структура СОА	335
7.4.2. Алгоритм работы ИИС на основе отрицательного отбора с применением нейросетевых детекторов	337
7.4.3. Особенности программной реализации алгоритма	340
7.4.4. Экспериментальная оценка эффективности ИИС	341
7.5. Построение искусственной иммунной системы для обнаружения компьютерных атак	345
7.5.1. Жизненный цикл детекторов иммунной системы	345
7.5.2. Функционирование иммунных нейросетевых детекторов	347
7.5.3. Алгоритм функционирования системы обнаружения вторжений на базе искусственных иммунных систем и нейронных сетей	350
Литература	352