

М. А. Полтавцева
Д. С. Лаврова

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ



М. А. Полтавцева, Д. С. Лаврова

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

2-е издание

*Рекомендовано Северо-Западным региональным отделением ФУМО
по информационной безопасности в качестве учебного пособия
для студентов высших учебных заведений,
обучающихся по УГСН 10.00.00 «Информационная безопасность»
по программам подготовки бакалавров, магистров, специалистов*

Москва Вологда
«Инфра-Инженерия»
2023

УДК 004.65
ББК 32.973.2
П52

Рецензенты:

ведущий научный сотрудник СПбФ АО «НИК "ТРИСТАН"»
д. т. н., профессор *Лебедев И. С.*;
зав. кафедрой защищенных систем связи СПбГУТ
к. т. н., доцент *Красов А. В.*

Полтавцева, М. А.

П52 Высокопроизводительные системы обнаружения вторжений : учебное пособие / М. А. Полтавцева, Д. С. Лаврова. – 2-е изд. – Москва ; Вологда : Инфра-Инженерия, 2023. – 152 с. : ил., табл.
ISBN 978-5-9729-1213-1

Рассмотрено построение высокопроизводительных систем обнаружения вторжений в компьютерных сетях и киберфизических системах. Приведены понятие и принципы обработки больших данных, архитектура систем высокой нагрузки, методы предобработки информации при обнаружении вторжений. Рассмотрены различные методы обнаружения вторжений, включая новые подходы на основе технологий искусственного интеллекта.

Для студентов, обучающихся по направлению «Информационная безопасность», и преподавателей, специализирующихся в области информационной безопасности. Может быть полезно широкому кругу специалистов, интересующихся вопросами обнаружения вторжений в системах с большим объемом циркулирующих данных.

УДК 004.65
ББК 32.973.2

ISBN 978-5-9729-1213-1

© Полтавцева М. А., Лаврова Д. С., 2023
© Издательство «Инфра-Инженерия», 2023
© Оформление. Издательство «Инфра-Инженерия», 2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	5
1. ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ ОБРАБОТКА ДАННЫХ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ	7
1.1. Большие данные и высоконагруженные системы	7
1.1.1. Эволюция данных и понятие Больших данных	7
1.1.2. Принципы и требования к обработке данных с высокой нагрузкой.....	11
1.1.3. Системы управления данными высокой нагрузки.....	16
1.1.4. Подходы к высокопроизводительной обработке данных	18
Контрольные вопросы и задания к разделу 1.1	22
Список источников к разделу 1.1	22
1.2. Технологии высокопроизводительной обработки данных	23
1.2.1. Пакетная обработка данных	23
1.2.2. Поточковая обработка данных.....	35
1.2.3. Принципы организации параллельного выполнения задач.....	65
1.2.4. Совместное использование потоковой и пакетной обработки	68
Контрольные вопросы и задания к разделу 1.2.....	76
Список источников к разделу 1.2	76
1.3. Обработка данных в задачах обнаружения вторжений.....	77
1.3.1. Типы данных и методы их обработки	77
1.3.2. Нормализация и агрегация данных из разнородных источников	82
1.3.3. Иерархическая агрегация данных.....	88
Контрольные вопросы и задания к разделу 1.3	92
Список источников к разделу 1.3	92
1.4. Параллельная организация вычислительного процесса.....	93
1.4.1. Обработка сообщений от устройств.....	93
1.4.2. Обработка сетевого трафика	98
1.4.3. Агрегация данных	101
Контрольные вопросы и задания к разделу 1.4.....	106
Список источников к разделу 1.4	106

2. МЕТОДЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ.....	107
2.1. Сигнатурные методы	108
2.1.1. Обнаружение вторжений на основе правил	109
2.1.2. Обнаружение вторжений на основе шаблонов	110
Контрольные вопросы и задания к разделу 2.1	111
Список источников к разделу 2.1	112
2.2. Поведенческие методы	112
2.2.1. Статистические методы для обнаружения вторжений.....	112
2.2.2. Энтропийный подход к обнаружению вторжений	119
2.2.3. Спектральный анализ для обнаружения вторжений	123
2.2.4. Фрактальный анализ для обнаружения вторжений	124
Контрольные вопросы и задания к разделу 2.2.....	127
Список источников к разделу 2.2	127
2.3. Методы искусственного интеллекта	128
2.3.1. Обнаружение вторжений на основе классификации	129
2.3.2. Обнаружение вторжений на основе кластеризации	136
2.3.3. Обнаружение вторжений с использованием машины Цетлина	138
2.3.4. Обнаружение вторжений на основе прогнозирования с использованием нейронных сетей	141
Контрольные вопросы и задания к разделу 2.3.....	143
Список источников к разделу 2.3	143
 БИБЛИОГРАФИЧЕСКИЙ СПИСОК	 146