

Оглавление

Предисловие	3
1. Компьютерные атаки	5
1.1. Основные определения и понятия	5
1.2. Классификация атак	6
1.3. Этапы реализации атак	8
1.3.1. Сбор информации	8
1.3.2. Основные механизмы реализации атак	10
1.3.3. Реализация атак	13
1.3.4. Завершение атаки	14
2. Принципы построения систем обнаружения вторжения	15
2.1. Классификация СОВ	15
2.2. Архитектура СОВ	25
2.3. Структура системы обнаружения вторжения	27
3. Технологии построения систем обнаружения атак	32
3.1. Существующие технологии СОВ	33
3.1.1. Технологии обнаружения аномальной активности	33
3.1.2. Анализ систем, использующих сигнатурные методы	35
3.1.3. Концепция обнаружения компьютерных угроз	38
3.2. Повышение эффективности систем обнаружения атак — интегральный подход	42
3.3. Характеристика направлений и групп методов обнаружения вторжений	44
3.4. Сравнительный анализ существующих СОВ	49
3.4.1. Bro	49
3.4.2. OSSEC	50
3.4.3. STAT	51
3.4.4. Prelude	53
3.4.5. Snort	55
3.4.6. SnortNet	58
3.4.7. AAFID	59
4. Анализ сетевого трафика и контента	63

4.1. Программы анализа и мониторинга сетевого трафика	63
4.1.1. Программы-анализаторы сетевого трафика	64
4.1.2. Обзор программ-анализаторов (снифферов) сетевого трафика	67
4.2. Получение и подготовка исходных данных для анализа свойств аномалий трафика	69
4.3. Анализ образцов трафика	71
4.3.1. Трассы и их анализ	73
4.3.2. Тестирование программного обеспечения	74
5. Анализ методов обнаружения аномалий	80
5.1. Статистические методы обнаружения аномального поведения	80
5.2. Ошибки первого и второго рода. ROC кривые	84
5.3. Критерии соответствия и однородности	87
5.4. Параметрический метод регистрации изменений	90
5.4.1. Контрольные карты	91
5.4.2. Контрольные карты Шухарта	93
5.4.3. Контрольные карты CUSUM	94
5.4.4. Контрольные карты EWMA	102
5.5. Критерии аномального поведения и их практическое применение	103
5.5.1. Процентное отклонение	104
5.5.2. Энтропия	108
5.6. Методы описательной статистики	108
5.7. Поиск и оценка аномалий сетевого трафика на основе циклического анализа	110
5.8. Обнаружение аномалий методом главных компонент	121
5.8.1. Основные положения метода главных компонент	121
5.8.2. Сингулярный спектральный анализ	129
5.8.3. Метод главных компонент и обнаружение аномалий	132
5.9. Достоинства и недостатки статистических методов	135
6. Обнаружение аномальных выбросов трафика методами кратномасштабного анализа	138
6.1. Основы теории вейвлетов	138
6.2. Непрерывное вейвлет-преобразование	139
6.3. Дискретное вейвлет-преобразование. Алгоритм Малла	141
6.4. Анализ методов обнаружения аномалий трафика с помощью вейвлетов	147

6.5. Алгоритм обнаружения аномалий методом дискретного вейвлет-преобразования	150
6.5.1. Алгоритм обнаружения аномалий по критерию Фишера для выбросов дисперсий	151
6.5.2. Алгоритм обнаружения аномалий на основе критерия Кохрана–Кокса	152
6.5.3. Алгоритм обнаружения аномалий по критерию Фишера для выбросов средних значений	153
6.5.4. Выбор порогов обнаружения	155
6.6. Дискретное вейвлет-пакетное преобразование	156
6.7. Обнаружение DoS- и DDoS-атак методами мультифрактального анализа	162
6.7.1. Фрактальные свойства телекоммуникационного трафика	162
6.7.2. Обнаружение DoS- и DDoS-атак методом мультифрактального анализа	166
7. Методы интеллектуального анализа данных в системах обнаружения вторжений	172
7.1. Методы Data Mining	172
7.2. Метод опорных векторов	175
7.3. Обнаружение аномалий трафика с применением нейронных сетей	182
7.3.1. Выявление аномалий сетевой активности с применением аппарата искусственных нейронных сетей	183
7.3.2. Применение нейронных сетей в задачах обнаружения вторжений	186
7.3.3. Архитектурные решения СОВ	187
7.3.4. Результаты экспериментов	190
7.4. Методы искусственного интеллекта в задачах обеспечения безопасности компьютерных сетей	192
7.4.1. Многоагентные системы	192
7.4.2. Системы анализа защищенности	193
7.5. Методы искусственных иммунных систем и нейронных сетей для обнаружения компьютерных атак	195
7.5.1. Построения искусственной иммунной системы для обнаружения компьютерных атак	195
7.5.2. Метод функционирования иммунных нейросетевых детекторов	197
7.5.3. Алгоритм функционирования системы обнаружения вторжений на базе искусственных иммунных систем и нейронных сетей	201
7.6. Визуальный анализ данных	203
7.6.1. Анализ методов визуализации	203

7.6.2. Использование преобразования Хафа для обнаружения аномалий трафика	207
7.7. Достоинства и недостатки методов обнаружения аномалий	209
Литература	212