**Алексеев Илья Вадимович Обнаружение распределённых атак отказа в обслуживании в крупномасштабных сетях на основе методов математической статистики и искусственного интеллекта**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Алексеев Илья Вадимович

ВВЕДЕНИЕ

1 Анализ угроз информационной безопасности в сети интернет от распределенных атак отказа в обслуживании и существующие методы их обнаружения

1.1 Примеры и особенности построения современных сетей

1.2 Анализ компонентов, входящих в состав топологий сетей

1.3 Анализ DDOS угроз ПО компонентов сети

1.4 Введение DDOS атак

1.5 Классификация DDOS атак

1.5.1 Объемные атаки

1.5.1.1 Атака UDP flood

1.5.1.2 Атака ICMP flood

1.5.2 Атаки на основе спецификации сетевых протоколов

1.5.2.1 Атака SYN flood

1.5.2.2 Атака с использованием IP-фрагментации

1.5.2.3 Атака RTP flood

1.5.3 Атаки на уровне приложений

1.5.3.1 Атака Slowloris

1.6 Механизмы реагирования на DDOS атаки

1.7 Выводы

2 Исследование существующих подходов и методов обнаружения ddos атак

2.1 Сигнатурные подходы к обнаружению DDOS атак

2.1.1 Анализ перехода состояний

2.1.2 Экспертные системы

2.1.3 Сети Петри

2.2 Методы, основанные на аномалиях

2.2.1 Статистический подход

2.2.2 Обнаружение на основе интеллектуального анализа данных

2.2.3 Подход, основанный на машинном обучении

2.3 Гибридные системы

2.4 Сравнительный анализ рассмотренных методов обнаружения и предотвращения DDOS атак

2.5 Проблемы при обнаружении DDOS атак для их предотвращения

2.6 Выводы

3 Подход к обнаружению ddos атак в крупномасштабных сетях на основе методов математической статистики и искусственного интеллекта

3.1 Вейвлет-преобразование для обнаружения аномалий

3.2 Исследование существующих подходов на основе вейвлет-преобразований

3.3 Предложенный метод метод двухступенчатой системы обнаружения DDOS атак в крупномасштабных сетях на основе отобранных параметров сетевых пакетов с использованием вейвлет-преобразования, методов математической статистики и искусственного интеллекта

3.4 Выводы

4 Прототип системы обнаружения ddos атак в крупномасштабных сетях и результаты экспериментальных исследований

4.1 Блок адаптации, обеспечивающий коррекцию параметров выполнения метода двухступенчатой системы обнаружения DDOS атак в крупномасштабных сетях относительно изменений интенсивности сетевой нагрузки и разнородности сети

4.2 Экспериментальные исследования

4.3 Выводы

ЗАКЛЮЧЕНИЕ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

ПРИЛОЖЕНИЕ А

ПРИЛОЖЕНИЕ Б

ПРИЛОЖЕНИЕ В

ВВЕДЕНИЕ